ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO

Trabajo de Tesis presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTORES:

MIREYA ELIZABETH RAMÍREZ QUINTERO

FABRICIO ALFREDO JIMÉNEZ CAICEDO

Riobamba-Ecuador

2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO

Trabajo de Tesis presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

AUTORES: MIREYA ELIZABETH RAMÍREZ QUINTERO
FABRICIO ALFREDO JIMÉNEZ CAICEDO

TUTOR: ING. VINICIO RAMOS VALENCIA MSc.

Riobamba-Ecuador

2016

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACONES Y REDES

El Tribunal de Tesis certifica que: el trabajo de investigación: "IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL TELEMONITOREO MÉDICO" de responsabilidad de la señorita Mireya Elizabeth Ramírez Quintero y el señor Fabricio Alfredo Jiménez Caicedo, ha sido minuciosamente revisado por los Miembros del Tribunal de Tesis, quedando autorizada su presentación.

	FIRMA	**FECHA**
Dr. Miguel Tasambay Ph.D **DECANO FACULTAD** **INFORMÁTICA Y ELECTRÓNICA**		
Ing. Franklin Moreno **DIRECTOR ESCUELA** **INGENIERÍA ELECTRÓNICA** **EN TELECOMUNICACIONES Y REDES**		
Ing. Vinicio Ramos **DIRECTOR DE TESIS**		
Ing. Janeth Arias **MIEMBRO DEL TRIBUNAL**		
NOTA		

Nosotros, Mireya Elizabeth Ramírez Quintero y Fabricio Alfredo Jiménez Caicedo somos responsables de las ideas, doctrinas y resultados expuestos en esta Tesis y el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo.

Mireya Elizabeth Ramírez Quintero

Fabricio Alfredo Jiménez Caicedo

DEDICATORIA

Dedico este trabajo a mi familia y amigos más queridos, especialmente a mis padres y hermanos quienes siempre estuvieron alentándome y dándome su apoyo incondicional en el intento por culminar una etapa más en mi vida.

Mireya

Al culminar esta etapa de mi vida que ha sido el resultado de mi esfuerzo, entrega y constancia, dedico este trabajo:

Primeramente, a Dios por brindarme la sabiduría y guiarme en cada uno de mis pasos, a mi madre Eugenia quien jamás me ha faltado y que siempre ha estado apoyándome pese a cualquier suceso, a mi familia, Alfredo y Mariana, por permitirme culminar exitosamente mi carrera.

Dedico a ellos todos mis éxitos y logros, por siempre brindarme el amor y la confianza, por ser quienes han estado conmigo siempre sin importar distancia ni circunstancia.

Para ellos que son parte de esta meta vayan los sinceros sentimientos de amor, respeto y admiración.

Fabricio

AGRADECIMIENTO

Agradezco a Dios por darme la sabiduría y la fuerza de continuar aún en los momentos más complicados, a mi familia en general por su apoyo incondicional en especial a mis padres por su esfuerzo y sacrificio incalculable de mantenerme en pie y alentarme a seguir, a mis hermanos por nunca retirarme su mano y demostrarme cuanto puedo contar con ellos, a mis pocos amigos quienes siempre estuvieron pendiente de mí y animándome a terminar esta etapa, a nuestro Director Vinicio Ramos por su guía y comprensión al compartir sus conocimientos y ayuda en conseguir un objetivo más.

Mireya.

Inicialmente agradezco a Dios por la fortaleza y valentía que me ha brindado para llegar hasta aquí, a mi madre quien ha sido el pilar fundamental en mi vida y a mi familia que son el mayor apoyo que he tenido; gracias a ellos por la confianza y la oportunidad de permitirme formarme como profesional.

Además, un abierto agradecimiento a la “Escuela Superior Politécnica de Chimborazo” y a la “Escuela de Ingeniería Electrónica en Telecomunicaciones y Redes” por abrirme sus puertas y así culminar con éxito esta gran etapa de mi vida.

Agradezco a mis docentes que supieron impartirme sus buenos conocimientos y que a la vez fueron amigos; a mis compañeros de clase y todas las personas que en algún momento me brindaron su apoyo sincero y de quienes me llevo un grato recuerdo.

Fabricio

TABLA DE CONTENIDOS

INDICE DE TABLAS

INDICE DE FIGURA

INDICE DE GRÁFICOS

INDICE DE ANEXOS

RESUMEN

El presente trabajo se efectuó con el objetivo de implementar un sistema de gestión de seguridad de la información aplicado al telemonitoreo médico. Para ello fue necesario la recopilación de información referente a redes inalámbricas de área corporal, el uso de la telemedicina en la sociedad y la relación con las TICs. Así mismo se analizó sobre la seguridad de red e información basada en la norma ISO 27001 para luego diseñar una estructura robusta que permita asegurar los datos transmitidos inalámbricamente, al mismo tiempo que se evaluaba e implementaba el sistema de Telemonitoreo médico. Fue preciso acudir al uso de placas electrónicas tales como Arduino UNO, Plataforma de sensores ehealth y módulo wifi 232-B para realizar el telemonitoreo. Una vez establecida la transmisión se realizó una categorización de activos y análisis y gestión de riesgos sobre el sistema representando así un porcentaje de cumplimiento de 71% de los requerimientos; además de realizar una comparación del sistema prototipo MFSecuEhealth contra un sistema no gestionado con seguridad obteniendo una mejora en el rendimiento notable de 86.2%. Se concluye que al analizar los requerimientos del sistema se logró optimizar los recursos y sobretodo se aseguró el activo más importante de la organización, la información. Se recomienda que para analizar, gestionar y monitorear un sistema informático se comparen los mejores gestores de seguridad para garantizar que su implementación salvaguarden las bases de la seguridad; confidencialidad, integridad y disponibilidad

PALABRAS CLAVES

<SEGURIDAD DE INFORMACIÓN>, <TELEMONITOREO MÉDICO>, <REDES INALAMBRICAS DE ÁREA CORPORAL [WBAN]>, <NORMA ISO 27001>, **<**INTEGRIDAD**>,** <CONFIDENCIALIDAD>, **<**DISPONIBILIDAD**>,** <OPTIMIZACIÓN DE RENDIMIENTO**>,** <TELECOMUNICACIONES**>**

ABSTRACT

This work is carried out with the objective of implementing a management system of information security applied to medical tele monitoring. This required the collection of information on wireless body area networks, the use of telemedicine in society and the relationship with ICTs. It was analyzed on security and based on the ISO 27001 and then design structure to ensure the data transmitted wirelessly while was evaluated and implemented the system of medical Tele monitoring. It was necessary to resort to the use of electronic boards such as Arduino UNO, ehealth platform sensors and wireless module 232-B for the monitoring. Once established transmission as set categorization, analysis and risk management of the system shown and a percentage of 71% compliance with the requirements is made; addition of a comparison against a prototype system MFSecuEhealth human aged system safely, obtaining a remarkable improvement in the yield of 86.2%. It is concluded that in analyzing the system requirements are managed to optimize resources and above all the most important asset of the organization and information is assured. It is recommended to analyze, manage and monitor a computer system best security managers are compared to ensure that its implementation will safeguard the foundations of security; confidentiality, integrity and availability

KEYWORDS

<INFORMATION SECURITY>, <MEDICAL TELEMONITORING>, <WIRELESS BODY AREA NETWORK (WBAN)>, <STANDARD ISO 27001 >, <INTEGRITY>, <CONFIDENTIALITY>, <AVAILABILITY>, < PERFORMANCE OPTIMIZATION>, <TELECOMUNICATIONS>

INTRODUCCIÓN

La presente investigación tiene por objeto implementar un ambiente de prueba en el cual se establezca un sistema de gestión de seguridad de la información aplicado al telemonitoreo médico de señales ECG (Electrocardiograma), Pulso y Porcentaje de oxígeno en la sangre a un individuo no crítico mediante el uso de sensores no invasivos.

El uso de la tecnología en todos los campos del conocimiento es innegable inclusive en el área médica. La medicina junto a las TICs (Tecnología de Información y Comunicación), se han encargado del desarrollo de una de las herramientas más importante actualmente, la Telemedicina. Esta herramienta abarca diferentes aplicaciones que satisfacen varias necesidades de la comunidad como un servicio ágil, oportuno y de calidad, confiable y sobre todo seguro.

Una de las aplicaciones de la Telemedicina es el Telemonitoreo; esta aplicación es de utilidad en gran parte para pacientes que requieren de un constante monitoreo de sus signos vitales y que por distintas razones no pueden acercarse al centro médico por lo que requieren enviar dichos datos usando las tecnologías inalámbricas disponibles hasta un servidor y de esta manera comprobar que se encuentran en los niveles correctos. Sin embargo, es importante saber que esta herramienta no es sustituta de procedimientos de asistencia o seguimiento presencial de un especialista.

En varios países del mundo tales como EE.UU., España, Francia, Australia, México, y algunos de Latinoamérica se ha logrado importantes avances tecnológicos en el ámbito de la Telemedicina, invirtiendo en Proyectos de Telesalud que permita brindar asistencia médica especializada, oportuna y a largas distancias.

Ecuador es unos de los países de América latina con mayores desigualdades en materia de salud y con menor inversión de recursos en esta área importante para su desarrollo, según la ONU. Sin embargo, en los últimos años se están invirtiendo en materiales de última tecnología adecuando instalaciones con el fin de ofrecer un mejor servicio de salud a la sociedad.

Justificación

Hoy en día el acceso a la salud es un factor fundamental que debe garantizar condiciones de atención apropiadas, ofreciendo servicios de salud con cobertura y calidad adecuados constituyendo una de las principales responsabilidades del estado y sociedades.

La tecnología presta servicios eficaces que se pueden utilizar en varias aplicaciones, explotando al máximo las herramientas que ahora se encuentran al alcance de toda persona, como es el Internet, teléfonos móviles, Tablet, computadoras, etc., las cuales son instrumentos de gran utilidad en actividades con mayor trascendencia.

La Telemedicina se introduce como una solución a un problema social, es decir una mejora en la calidad actual de atención médica llegando a todos los lugares del país, inclusive a los más lejanos.

El Telemonitoreo médico es una aplicación basada en redes de área corporal, consiste en el uso de sensores ubicados bajo la piel (implantados) o en la superficie de la misma facilitando la adquisición de información del cuerpo humano. Para el desarrollo de este proyecto se tomarán las señales de signos vitales, tales como; ritmo cardiaco, pulso y nivel de oxígeno en la sangre, los mismos que serán enviados inalámbricamente (WiFi).

Debido a que la transmisión se realiza inalámbricamente y teniendo en cuenta la importancia y sutileza con la que se debe manejar la información, es necesario tomar las medidas de seguridad que garanticen la continuidad de las actividades en el caso que se produzcan incidencias, fallos o actuación malintencionada por parte de terceros salvaguardando la integridad, confidencialidad y disponibilidad de dichos datos.

Este proyecto se realizó con el interés de implementar un sistema que optimice tiempo y recursos, en primer lugar, en telemonitoreo en el cual se manejan datos en tiempo real por lo cual se deben considerar aspectos técnicos como el retardo en la transmisión, y en segundo lugar en la gestión de seguridad. La seguridad de la información hoy en día es de mucha importancia en organizaciones de todas las áreas de trabajo debido a la protección que se da a sus activos; como consecuencia implementar un sistema de gestión de seguridad eficiente contra amenazas informáticas es una de las prioridades de toda entidad.

Es evidente que el sistema a desarrollar en un *Ambiente de Prueba* será de mucha utilidad en la sociedad, ya que se demostrará a plenitud que es un sistema factible al contar con la tecnología necesaria para cualquier persona y además se podrá dar ayuda oportuna a quien lo necesite con mayor rapidez, evitando así resultados inesperados que puedan perjudicar al paciente y al profesional médico.

Para robustecer el sistema de seguridad se implementará un Sistema de Prevención de Intrusos (IPS) que permita el control de acceso no autorizado a la red para garantizar el uso responsable

y profesional del mismo que beneficie únicamente a los pacientes de alguna enfermedad que pueda ser tratada a distancia y de forma urgente, que inclusive incluye la realización de intervenciones quirúrgicas de emergencia que pueden salvar vidas.

De igual manera se deben describir las políticas de seguridad necesarias para el buen funcionamiento del sistema y evitar accesos no autorizados y manipulación de información sensible del paciente tratado.

Debe destacarse que por el momento este Ambiente de Prueba será de utilidad como experimentación en tanto puedan contar las unidades hospitalarias o los consultorios de los profesionales de la medicina con los recursos técnicos necesarios para poder implementar este novedoso sistema de atención médica que está revolucionando este campo tan necesario para la prevención y curación de enfermedades que causan graves trastornos en la salud del hombre.

Objetivos

Objetivo General

"Implementar un sistema de gestión de seguridad de la información aplicado al Telemonitoreo Médico."

Objetivos Específicos

- Investigar la información necesaria sobre las redes inalámbricas de área corporal (WBAN), el uso de la Telemedicina en la sociedad y su relación con las TICs.

- Diseñar una estructura de seguridad robusta que permita asegurar la información basándose en la norma ISO 27001.

- Implementar una guía de políticas de seguridad que garanticen la protección de red e información del sistema.

- Evaluar e implementar en un ambiente de prueba un Sistema de Telemonitoreo médico y la seguridad sobre los datos.

En el marco metodológico se realizó un diseño investigativo en tres fases para alcanzar los objetivos propuestos. La fase de análisis general en el cual se estudiará el estado actual de la

atención hospitalaria a personas geográficamente distantes, además de la importancia de seguridad de la información en este aspecto. En la fase de desarrollo del proyecto se recopilará información sobre seguridad basándose en la norma ISO 27001. Por último, la fase de pruebas de implementación en el cual una vez desarrollado el ambiente de prueba se comprobará la eficiencia de las reglas efectuadas en el sistema de seguridad Sophos.

El tipo de investigación es descriptiva-aplicada ya que se propone una solución a un problema aplicando conocimientos y estableciendo estrategias o una guía de proceder que garantice una atención eficaz además de la seguridad de los datos.

Los métodos empleados para el desarrollo de este proyecto son: documental o teórico y de campo. Esto indica que se realizó una recolección teórica y a partir de eso se aplica un ambiente de prueba.

Las técnicas a utilizar son: observación, recopilación teórica, análisis de contenidos y pruebas sobre la implementación. Estas pruebas se realizan en individuos al azar con el fin de comprobar la transmisión en tiempo real de los datos y evaluar los principios básicos de la seguridad: confidencialidad, disponibilidad e integridad.

Para lograr la comunicación entre los sensores y la PC, se utilizarán herramientas electrónicas tales como Plataforma de Sensores ehealth sobre el que se conectaran los sensores que tomaran las señales biomédicas, Arduino UNO en la que configurará el modo de trabajo para transmitir los datos, módulo wifi 232 que servirá para la comunicación inalámbrica. Una vez se establezca dicha conexión la información transmitida se almacenará en un servidor central, a la cual podrán ser accedidos desde cualquier lugar.

La seguridad se realizará con el uso de un sistema robusto como lo es Sophos, en él se aplicará las reglas permitidas y restringidas para el acceso a los datos del sistema. A más de aplicar definiciones de usuarios reglas y políticas de red, protección inalámbrica, VPN, IPS, Servicios de autenticación, entre otros.

CAPÍTULO I

1. MARCO TEÓRICO REFERENCIAL

1.1 Red Inalámbrica de Área Corporal (WBAN)

1.1.1 Definición

Wireless Body Area Network o Red Inalámbrica de Área Corporal (WBAN) es una red inalámbrica de dispositivos portátiles de baja potencia de propósito especial diseñado para funcionar de manera autónoma conectando varios sensores médicos y aplicaciones, localizados en la ropa, sobre el cuerpo o bajo la piel de una persona con la finalidad de obtener datos fisiológicos o registro de la actividad física.

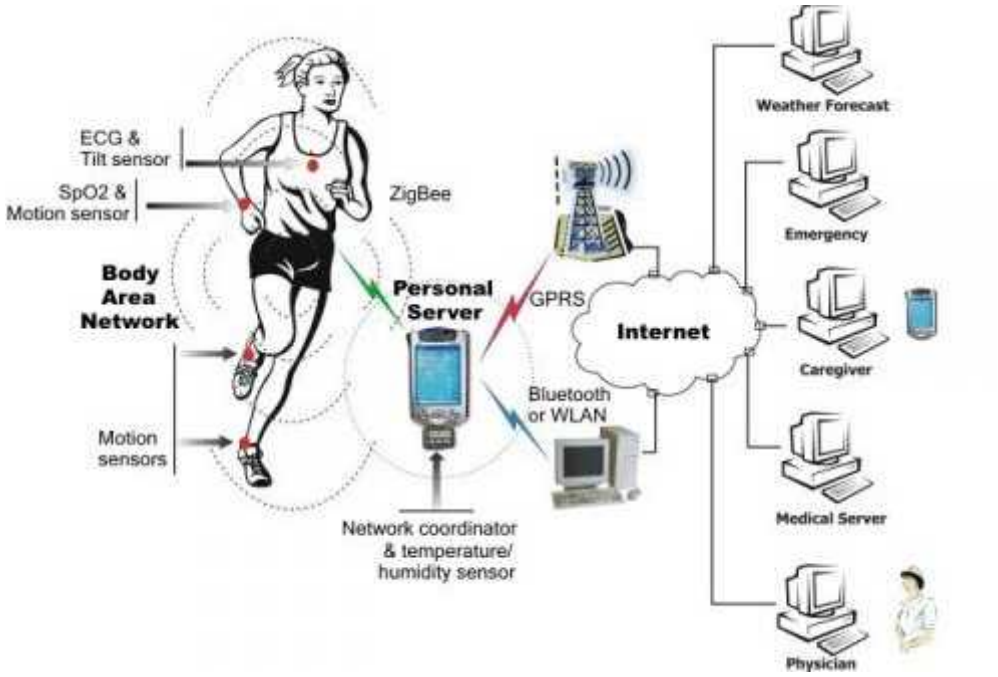


Figura 1-1: Red Inalámbrica de Área Corporal

Fuente: Jtel, 2008

En la figura 1-1 se muestra un escenario donde se accede remotamente a los datos de un grupo de sensores.

Las redes WBAN son consideradas una tecnología reciente derivada de las redes WSN (Red Inalámbrica de sensores); pese a esto, su proceso de desarrollo es notable en muchos campos aplicativos especialmente en la medicina, esto se debe a la facilidad que presta en la obtención y transmisión de datos mejorando la monitorización de pacientes.

1.1.2 Arquitectura de una Red Inalámbrica de Área Corporal

La arquitectura de una red WBAN consiste en nodos sensores y nodo coordinador llamado también servidor personal o Gateway. En la figura 2-1 se indica el modo de operación de una WBAN teniendo los sensores y el coordinador conectados mediante enlace inalámbrico.

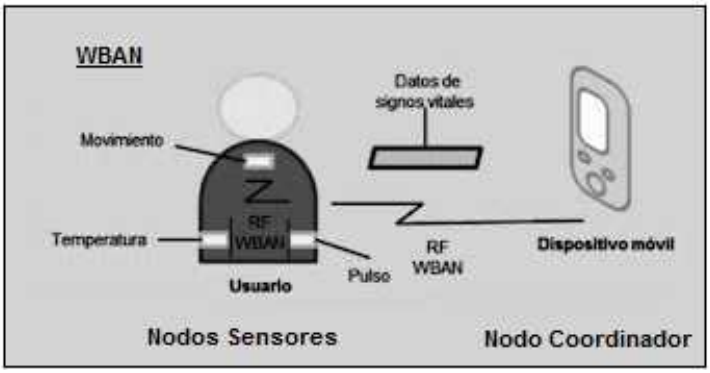


Figura 2-1: Arquitectura de una red WBAN

Fuente: Diana Patricia Tobón Vallejo & Natalia Gaviria Gómez, 2010, p 43

1.1.2.1 Nodo Sensor

Los sensores constituyen una parte importante en este tipo de red. Debido al contacto directo que tienen con el cuerpo humano ya sea bajo la piel o sobre ella; el tamaño y compatibilidad con los tejidos del cuerpo son críticos. El nodo sensor puede estar compuesto por una variedad de sensores fisiológicos, esto dependerá de la aplicación final de la red.

Con el avance tecnológico se han desarrollado una variedad de sensores, cada vez mejorando ciertas características relevantes que se deben considerar en dichos dispositivos, tales como; el procesamiento de señales, transmisión, potencia, calidad, portabilidad, entre otras.

Figura 3-1: Nodo Sensor

Fuente: Cooking Hacks: Biometric /Medical Applications. 2013

Los nodos sensores se encuentran en un constante funcionamiento. Recopilan, procesan y almacenan información en su memoria interna, y posteriormente es enviada al coordinador o gateway.

Estos dispositivos están constituidos por varias partes: módulo de censado, módulo de radiofrecuencia, módulo de memoria y módulo de microprocesador. Además, en ciertos casos incluyen un módulo de almacenamiento y generación de energía. Figura 4-1

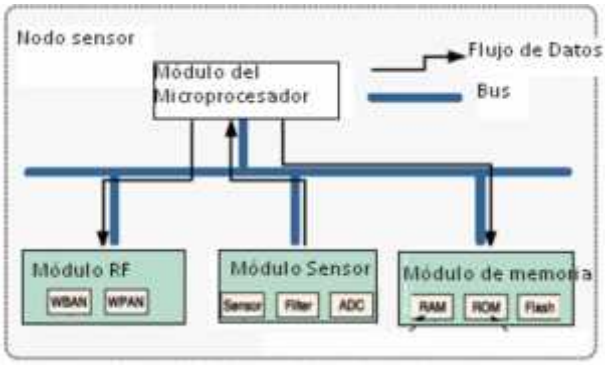


Figura 4-1: Arquitectura Nodo Sensor

Fuente: María Fuentes y Anthony Cedeño, 2010, p 35

"El módulo sensor responsable de la recolección de los datos fisiológicos; consiste principalmente de un sensor, un filtro y convertidor analógico/digital, el sensor convierte la señal fisiológica en señal eléctrica, después de lo cual la señal pasa por un filtro pasa banda y se digitaliza mediante el convertidor analógico digital. Esta información se procesa y se almacena en memoria, tras lo cual se envía con la ayuda del módulo de radiofrecuencia al nodo coordinador, obteniendo su energía de baterías o de generadores propios" (Alvarado & Juárez, 2012, p 27).

1.1.2.2 Nodo Coordinador

Es cualquier dispositivo que sirva de comunicación entre los nodos sensores, es un nodo único responsable de las siguientes tareas: inicialización, configuración, sincronización, control y operación de los nodos sensores, recopilación, procesamiento e integración de datos de varios sensores fisiológicos para proporcionar al usuario facilidad de lectura e interpretación sobre su estado, también se encarga de la comunicación con los servidores remotos de atención médica utilizando las diferentes tecnologías de comunicación inalámbrica.

La aplicación que interpreta los datos recopilados puede ser instalada en cualquier dispositivo móvil (PDA, teléfono celular o computador personal), la misma que recepta la información enviada por los nodos sensores mediante un enlace inalámbrico. Dicho coordinador debe tener la disponibilidad de conexión a Internet en caso que se requiera la transmisión de datos a un servidor remoto de servicio médico como se muestra en la figura 5-1.

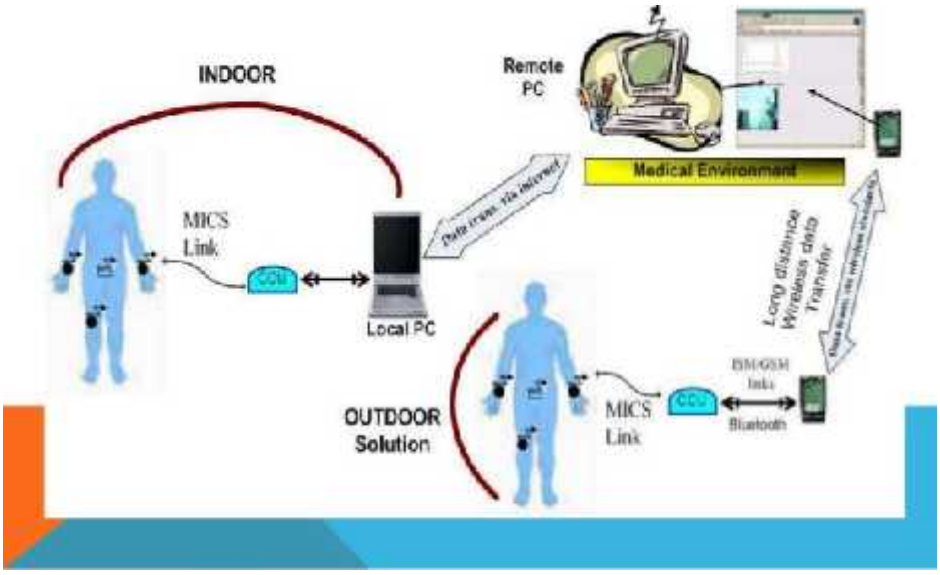


Figura 5-1: Conexión de Nodos Sensores a Nodo Coordinador

Fuente: Jorge Luis Nava, 2013

1.1.3 Modo de Operación

1.1.3.1 Sistema Operativo

Debido a la aplicación que tienen estos dispositivos y los requerimientos con los que debe cumplir (tamaño físico, lógico, optimización de potencia y carga) el sistema operativo utilizado debe ser de baja complejidad con respecto a los sistemas de propósito general, es por ello que gran parte de estos sensores funcionan con el sistema operativo (SO) TinyOS.

“Este es un SO de código abierto basado en responder a características y necesidades de la red de sensores tales como reducido tamaño de memoria, bajo consumo de energía, operaciones de concurrencia intensiva, diversidad en diseños y usos, y finalmente operaciones que facilitan el desarrollo confiable de aplicaciones. Además, se encuentra optimizado en términos de uso de memoria y eficiencia de energía” (Alvarado & Juárez, 2012, p 37).

1.1.3.2 Enrutamiento

En redes de área corporal el objetivo del enrutamiento es la reducción de la absorción de energía en el cuerpo humano, tomando en cuenta esta consideración las formas de enrutamiento son:

- Enrutamiento por agrupación: Se utiliza el algoritmo LEACH, el cual mediante una combinación de protocolo jerárquico y una rotación aleatoria de nodos se convierte en el método idóneo para ser aplicado en redes de gran escala.
- Enrutamiento consiente de la temperatura: La Tasa de Absorción Especifica (SAR) indica la cantidad de energía de radiación que es absorbida por el cuerpo. Este es un aspecto que debe tenerse en cuenta en las redes WBAN al momento de implementar el enrutamiento de nodos. Por otro lado, también se podría considerar la temperatura para seleccionar las rutas.
- Enrutamiento en nodos implantados: En este tipo de redes las restricciones son aún mayores, debido a la absorción de energía en el tejido del cuerpo por lo cual es necesario la implantación de un nodo coordinador, el cual servirá de guía para para la transmisión de datos a un nodo de mayor distancia con lo cual se previene la perdida de información.

1.1.3.3 Interoperabilidad

La cobertura de una WBAN se limita a pocos metros (2m a 5m), sin embargo, esta distancia se puede incrementar con el uso de otras redes inalámbricas que permitan expandir la conectividad entre sensores llegando así a transmitir información hasta un dispositivo de mayor capacidad de gestión y almacenamiento indicado en la Figura 6-1.

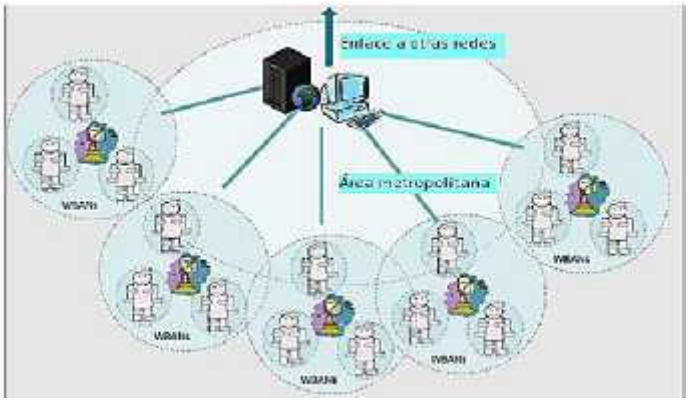


Figura 6-1: Interconexión de redes WBAN con otras redes

Fuente: María Fuentes y Anthony Cedeño, 2010, p 49

1.1.4 Aplicaciones de una Red Inalámbrica de Área Corporal

En la actualidad existe una gran variedad de sensores que se están desarrollando, por lo cual las aplicaciones variaran de acuerdo al tipo de sensor utilizado. Entre las aplicaciones que han sido ideadas para estas redes, se encuentra: la vigilancia de pacientes en el hogar, seguimiento y análisis de atletas, entre otros.

1.1.4.1 Aplicaciones Médicas

Las redes WBAN representan una excelente herramienta en el ámbito médico, especialmente para el diagnóstico y monitoreo de pacientes en escenarios como hospitales y hogares, proporcionando facilidad en la generación de alarmas y servicios de emergencia, así como la gestión de base de datos y nuevos registros.

En la figura 7-1 se expone un sistema donde se tienen nodos de redes WBAN configurados para enviar alertas de emergencias mediante las aplicaciones en una infraestructura médica.

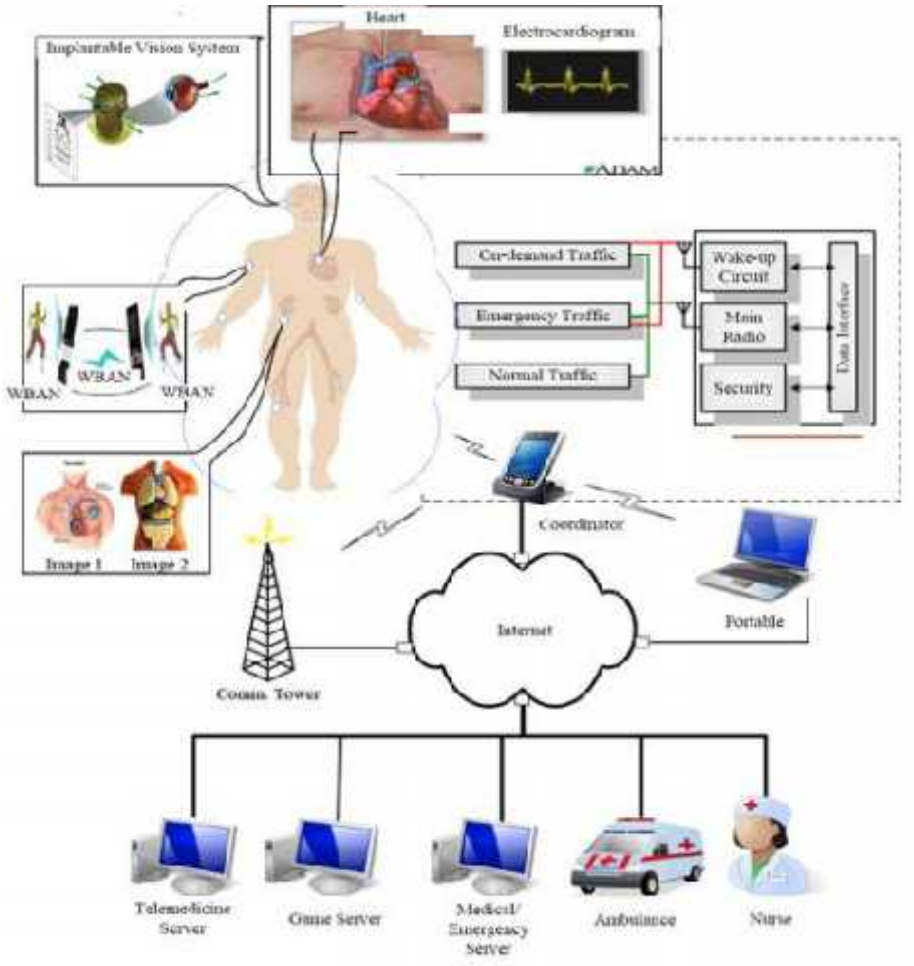


Figura 7-1: Redes WBAN en aplicaciones médicas

Fuente: John Bustamante Osorno, J. F. Sáenz, A. A. Amaya, 2011

1.1.4.2 Aplicaciones Deportivas

Con el uso de sensores colocados en diferentes áreas del cuerpo se podrá tomar registros de signos vitales de personas que se encuentran en constante actividad física, con el fin de identificar posturas y movimientos específicos. Con esta tecnología, se puede mejorar su rendimiento y evitar lesiones por posturas incorrectas, monitorear al deportista y medir sus cualidades físicas, su respuesta ante esfuerzos y todo tipo de información relativa a su estado físico.

1.1.4.3 Aplicaciones Militares

"Las redes WBAN empleadas en aplicaciones militares brindan importantes funciones, como: la distribución y consumo adecuado del agua, la reducción de daño corporal debido a condiciones ambientales adversas, y mejorar la calidad de atención médica en el caso de algún daño. Para

alcanzar estos objetivos, el GPS y la información fisiológica del sensor se transmite a través de sistema de red WBAN, cuyo diseño debe incluir los sensores fisiológicos, modelos predictivos, algoritmos e interfaces de usuario" (Alvarado & Juárez, 2012, p 64).

1.2 Telemedicina

Actualmente la Telemedicina se considera un servicio útil, no solo en lugares apartados geográficamente, sino también en medios urbanos en donde la ampliación y mejora de varios aspectos y procesos de asistencia médica han sido fundamentales para el desarrollo y evolución de instituciones hospitalarias.

Hoy en día gracias a las aportaciones tecnológicas de las TICs, existe una poderosa interacción médico – paciente, lo cual mejora y facilita el seguimiento médico independientemente del lugar donde se encuentre, además de permitir la educación sanitaria, administración y gestión de pacientes.

1.2.1 Definición

La Telemedicina es el término dado a la práctica de la medicina a distancia. Permite dar asistencia y seguimiento médico a pacientes sin importar la ubicación geográfica ya sea del médico tratante o de la persona tratada. Además, es usada como herramienta interactiva para consultas entre profesionales médicos y de forma educativa en videoconferencias. En este ámbito en el que la distancia y el tiempo de respuesta representan un factor crítico, deben intervenir tecnologías avanzadas de telecomunicación, que permitan un tratamiento y trasmisión de la información confiable y segura; es por ello el uso de TICs.

Figura 8.1: Integración de la Telemedicina

Fuente: Anna Martínez., 2010

En la figura 8-1 se interpreta la integración de un segmento de las telecomunicaciones con ciertas ramas de la medicina.

1.2.2 Aplicaciones de la Telemedicina

La Telemedicina tiene múltiples aplicaciones, las cuales van mejorando con el avance de la tecnología, con el fin de optimizar los recursos y maximizar su potencial de utilidad.

1.2.2.1 Teleconsulta

La Teleconsulta puede ser en tiempo real y diferido. En tiempo real se realiza desde el centro de salud rural hasta el hospital de referencia mediante videoconferencia o video llamada. En la Teleconsulta diferida, se realiza el almacenamiento de la información necesaria del paciente y posteriormente es enviada al hospital para ser remitida al médico especialista. El médico especialista deberá dar una respuesta en un tiempo mínimo menor a 24 horas.

1.2.2.2 Telediagnóstico

Se realiza al enviar a través de internet los datos del paciente adjuntando imágenes con el fin de diagnosticar y tener una amplia visión del paciente por medio de ellas. Actualmente se realiza, telediagnóstico general, telediagnóstico por imágenes, teleradiología, teledermatología, teleoftalmología, telepatología, telecitología, teleendoscopía.

1.2.2.3 Teleterapia

Se refiere a la realización de tratamientos y consultas de pacientes haciendo uso de herramientas de videoconferencia, esto incluye además el manejo de equipos a distancia.

1.2.2.4 Teleeducación

Se entiende por Teleeducación al proceso de enseñanza a distancia que se imparte mediante el uso de tecnología de información y comunicación. Esta puede ser de dos tipos: unidireccional y bidireccional. La primera se da cuando los participantes reciben la capacitación, curso o plática sin poder preguntar o intervenir sobre el tema. La segunda es cuando existe una interacción entre el expositor y los participantes

1.2.2.5 Telemonitoreo

La telemonitorización, permite obtener los signos vitales de un paciente de forma continua y permanente evitando el desplazamiento hasta el centro de salud para ello; esto es posible ya sea; por llamadas telefónicas por parte del personal de salud, con el uso de sensores permanentes o incluso comunicándose los mismos pacientes al servidor web, de esta forma los médicos podrán revisar el estado del paciente mediante una conexión a la intranet de hospital.

Dentro de las funciones de la telemonitorización, se encuentra, el llevar un control constante de embarazadas, personas con enfermedades crónicas, deportistas, etc., además de la telemetría (tele-cardiología, tele-oftalmología, tele-neurología, tele−radio seguridad, tele−bioseguridad).

Es importante indicar, que el telemonitoreo, es una herramienta de apoyo para el tratamiento, y no un sustituto de procedimientos de asistencia o seguimiento presencial.

1.2.3 Relación entre la Telemedicina y las TIC's

El desarrollo, integración y convergencia de las diferentes tecnologías de la comunicación han dado lugar a las Tecnologías de la Información y Comunicación (TIC). Dado su alcance y aplicación en todas las áreas de desarrollo incluida la Telemedicina, es importante el estudio de su relación con la misma, de esa manera se entenderá el rol que desempeña en el avance de todas las áreas de aplicación que abarca esta herramienta útil de sobremanera para la sociedad.

El uso de las TICs en la Telemedicina constituye una potente herramienta, lo cual ayuda al logro de los objetivos de salud propuestos por la organización médica en beneficio de la comunidad. Los identificadores que se logran mejorar con el uso de las tecnologías son: acceso, eficacia, eficiencia, calidad, seguridad, generación de conocimiento, impacto en la economía e integración; cada uno de ellos vinculados a las distintas áreas de aplicación de la telemedicina.

Sin embargo, para que esto sea efectivo es condición necesaria avanzar, de manera coherente y sostenida, en el desarrollo de infraestructura e implementación de aplicaciones, validadas e interoperables, tanto en los ámbitos de la educación sanitaria como de la prevención de enfermedades, de la asistencia médica y de la gestión de los servicios.

1.3 Sistema de Comunicación

El propósito del sistema de telemonitoreo es la conexión de dispositivo sensor que tomará datos de signos vitales en un paciente remoto y lo transmitirá vía wifi a un servidor central, al cual personas autorizadas podrán acceder para realizar el respectivo seguimiento. Para desarrollar esto, se tienen dos opciones; se puede diseñar toda la red sobre una red pública o se puede diseñar una red privada para conexión sensor-servidor y el acceso se haga mediante el internet.

La primera opción, aunque es sencilla debido a que tanto el sensor como el servidor se conectan a Internet no prestaría mucha seguridad. En la segunda opción el sensor remoto se conecta al servidor a través de una red privada, y el acceso al mismo se debe hacer a través de una red pública. Esta opción hace que se conserve un nivel de seguridad mayor que en la primera al tener un canal privado y dedicado entre los sitios.

Habiendo comparado las dos opciones, se implementará la segunda opción, ya que nos proporcionará mayor seguridad y disponibilidad.

1.3.1 Comunicación Inalámbrica WiFi

1.3.1.1 Generalidades

Llamada también WLAN (Wireless Lan) es una de las tecnologías de comunicación inalámbrica más utilizada hoy en día estandarizada por la IEEE (Instituto de Ingenieros en Electricidad y Electrónica) bajo las normas 802.11.

Tabla 1-1: Estándares aplicado por la IEEE en Redes Inalámbricas

Nombre	Tecnología	Velocidad de Transmisión	Características
Wireless B	IEEE 802.11b	11 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente, compatible con velocidades menores.
Wireless G	IEEE 802.11g	11/22/54 Mbps	Trabaja en la banda de frecuencia de 2.4 GHz solamente.
Wireless N	IEEE 802.11n	300 Mbps	Utiliza una tecnología denominada MIMO (que por medio de múltiples antenas trabaja en 2 canales), frecuencia 2.4 GHz y 5 GHz simultáneamente.
Wireless AC	IEEE 802.11ac	433 Mbps/1.3 Gbps	Trabaja sobre la banda de los 2.5 Ghz a 5 Ghz (MIMO) de 3 canales, múltiples antenas, también llamada Wi-Fi 5/5G

Fuente: www.informáticamoderna.com, 2010

Las redes inalámbricas transmiten a velocidad de 11Mbps o superior proporcionando la rapidez y movilidad necesaria para el funcionamiento de una gran mayoría de aplicaciones. Al hablar de transmisión inalámbrica es indispensable tener en cuenta la seguridad de la información, ya que cualquier persona podría interceptar la comunicación y darle un uso indebido a los datos obtenidos por lo cual la transmisión debe ser encriptada.

1.3.1.2 Módulo Wifi232-B

Es un dispositivo que permite la transmisión inalámbrica de datos a cualquier equipo. El módulo recepta los datos y realiza un proceso de conversión para establecer la comunicación ya sea TCP o UDP. La configuración se puede realizar vía comandos o por acceso web.

Figura 9-1: Módulo wifi 232-b

Fuente: www.Alibaba.com, 2012

Éste es un dispositivo utilizado en numerosas aplicaciones de alto rendimiento tales como:

- Monitoreo de Equipo Remoto
- Sensores y Controles Industriales
- Domótica
- Dispositivos médicos

Tabla 2-1: Especificaciones Generales del módulo wifi232-b

Categoría	Detalle	Parámetro
Parámetros Wireless	Certificación	FCC/CE
	Estándar Wireless	802.11 b/g/n
	Rango de Frecuencia	2.412GHz-2.484GHz
	Potencia de Transmisión	802.11b: +20 dBm (Max.)
		802.11g: +18 dBm (Max.)
		802.11n: +15 dBm (Max.)
		Configurable
	Sensibilidad del Receptor	802.11b: -89 dBm
		802.11g: -81dBm
		802.11n: -71dBm
	Opción de Antena	Externo: Conector I-PEX
		Interno: Antena incluida
Parámetros de Hardware	Interface de datos	UART: 1200bps - 230400bps
		GPIOs
		Ethernet: 100Mpbs
	Voltaje de Funcionamiento	3.3V (+/-5%)
	Corriente de funcionamiento	170mA~300Ma
	Temperatura de Funcionamiento	-25℃- 85℃
	Temperatura de almacenamiento	-40℃- 125℃
	Dimensiones y Tamaño	25×40×8mm
Parámetros de Software	Tipo de red	Estación /AP modo/STA+AP
	Mecanismos de Seguridad	WEP/WAP-PSK/WAP2-PSK/WAPI
	Encriptación	WEP64/WEP128/TKIP/AES
	Modo de Trabajo	Transmisión Transparente
	Línea de Comandos	AT+ instruction set
	Protocolo de red	TCP/UDP/ARP/ICMP/DHCP/DNS/HTTP
	Max. Conexiones TCP	32
	Configuración de usuario	Web Server + AT command.

Fuente: www.waferstar.com

1.3.2 Arduino Uno

Es una placa electrónica de código abierto que contiene un microcontrolador marca Atmel además de la circuitería necesaria para su funcionamiento y un Entorno de desarrollo integrado (IDE). Tiene 14 pines que pueden ser configurados como entrada o salidas digitales, de las cuales 6 pueden son utilizadas como salidas PWM (Modulación por ancho de pulsos) y a las que se puede conectar cualquier dispositivo capaz de recibir o transmitir señales.

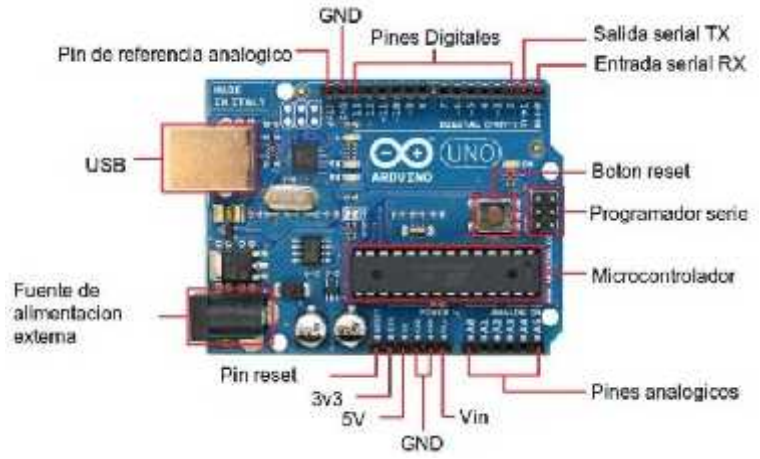


Figura 10-1: Estructura de Arduino UNO

Fuente: www.arduino.cc, 2012

En la figura 10-1 se puede apreciar la estructura de un Arduino UNO. Esta placa se configura a través de un cable USB que viene incluido en el kit, este se conecta a la computadora y se procede con la configuración del mismo considerando librerías y demás funciones que permitan su correcto funcionamiento.

Al conectar la placa Arduino UNO a la computadora debemos verificar el COM que se crea, ya que es el puerto serial que servirá para su configuración y por ende para la visualización de datos transmitidos.

La programación de Arduino es realizado en Lenguaje C / C++ y basado en Wiring, lo que permite desarrollar programas ejecutables.

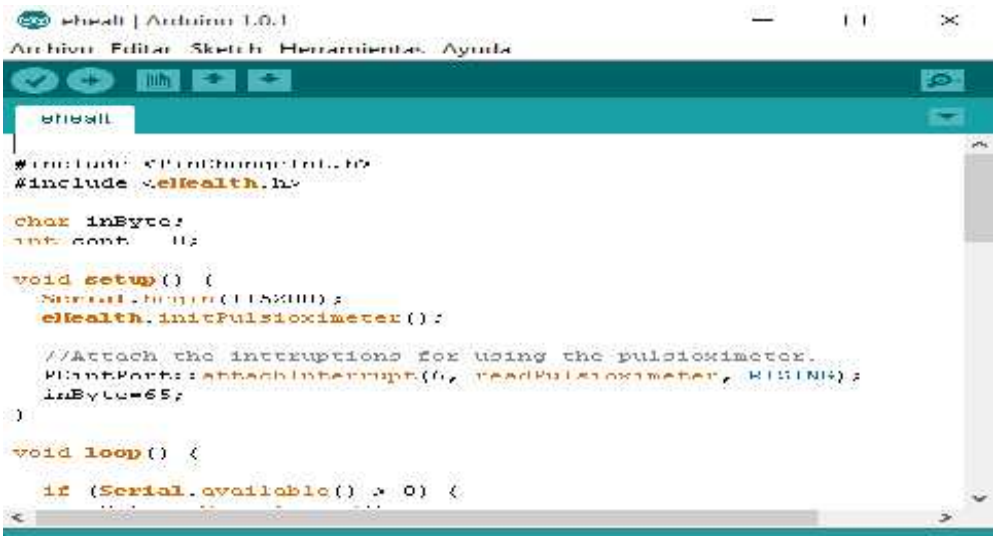


Figura 11-1: Programación de Arduino UNO de la toma de señales biomédicas

Realizado por: M. Ramírez y F. Jiménez, 2015

En la figura 11-1 se exhibe la interfaz gráfica para programar Arduino.

Debido a su utilidad en varias áreas Arduino se puede ejecutar en Windows, Mac OS y Linux utilizando las versiones respectivas para cada sistema operativo. Sus especificaciones técnicas se describen en la Tabla 3-1.

Tabla 3-1: Características técnicas de Arduino

Microcontrolador	Atmega328
Voltaje de operación	5V
Voltaje de entrada (Recomendado)	7 – 12V
Voltaje de entrada (Limite)	6 – 20V
Pines para entrada- salida digital.	14 (6 pueden usarse como salida de PWM)
Pines de entrada analógica.	6
Corriente continua por pin IO	40 mA
Corriente continua en el pin 3.3V	50 mA
Memoria Flash	32 KB (0,5 KB ocupados por el bootloader)
SRAM	2 KB
EEPROM	1 KB
Frecuencia de reloj	16 MHz

Fuente: www.arduino.cc, 2014

1.3.3 Plataforma de sensores eHealth

Es una plataforma que usa Arduino y Raspberry desarrollada por Cooking Hacks para llevar a cabo aplicaciones médicas y biométricas donde la monitorización es esencial. En ésta se pueden usar 10 diferentes sensores tales como: pulso, oxígeno en sangre (SPO2), flujo de aire en la respiración, temperatura corporal, electrocardiograma (ECG) glucómetro, sensor galvánico de respuesta de la piel, presión sanguínea, posición del paciente (acelerómetro) y sensor electromiográfico, que se puede indicar en la figura 12-1

Toda la información obtenida por los sensores puede ser usada por un especialista para monitorización en tiempo real de un paciente en forma remota. Dicha información se transmitirá mediante cualquiera de las siguientes opciones: Wi-Fi, 3G, GPRS, Bluetooth, ZigBee 802.15.4

Figura 12-1: Conexión de sensores a plataforma e-health

Fuente: www.cooking-hacks.com, 2013

1.3.4 Sensores médicos

Lo sensores recopilan y transmiten la información que obtienen del cuerpo para que sea procesada, interpretada y enviada. Las instituciones de salud requieren resultados de diagnósticos fiables y precisos en tiempo real proporcionados por dispositivos que se pueden supervisar de forma remota, por si el paciente se encuentra en un hospital, en una clínica o en casa.

Estos sensores pueden ser invasivos y no invasivos. Invasivos en el caso de ser implantados bajo la piel de una persona, no invasivos cuando se colocan sobre la piel o la ropa.

1.3.4.1 Pulsioximetro

Es un dispositivo que permite la medición no invasiva de la cantidad de oxígeno que se combina con la sangre para formar la oxihemoglobina, el cual es el elemento que transporta el oxígeno hacia los tejidos.

Los niveles normales de saturación de oxígeno se encuentran entre 96% y 99%. Si el porcentaje se encuentra por debajo del 90% se produce hipoxemia, es decir disminución anormal de la presión parcial de oxígeno en sangre arterial.

Figura 13-1: Pulsioxímetro

Fuente: www.medicaexpo.es, 2014

Este dispositivo se coloca sobre una zona translucida del cuerpo (yema del dedo, lóbulo del pabellón auricular, etc) emitiendo luz de distintas longitudes de onda; roja (660nm) e infrarroja (940nm) y mide como la sangre arterial absorbe cada longitud de onda, ofreciendo así una lectura del nivel de oxígeno.

Los valores de pulso normales se encuentran entre 60 y 100 pulsaciones por minuto. Si el valor está sobre las 100 pulsaciones por minuto se produce Taquicardia y si las pulsaciones son menores a 60 se produce Bradicardia.

1.3.4.2 Electrocardiograma

"Representación gráfica de la actividad eléctrica del corazón y del ritmo cardíaco. Se usa para el diagnóstico de enfermedades cardiovasculares. El electrocardiograma (ECG) también se utiliza para estudiar posibles alteraciones cardíacas durante la realización de un esfuerzo físico o de una actividad fisiológica como el sueño" (Enciclopedia salud, 2013)

Figura 14-1: Electrocardiograma ECG

Fuente: www.cookinghacks.com, 2014

Para realizar un electrocardiograma se utilizan electrodos que permiten medir las señales. Su función es convertir las señales iónicas producidas por los tejidos en señales que puedan ser

interpretadas por los usuarios. Generalmente los datos expulsados son voltajes que varían de acuerdo a la actividad en la que se encuentre el individuo.

1.3.5 Esquema General del Sistema

El sistema de telemonitoreo médico se planteará en un ambiente de prueba utilizando dispositivos diseñados para fines experimentales. Para su desarrollo se utilizará la plataforma de sensores e-health y una placa arduino, en la cual se programará la lectura de datos desde los sensores para luego ser transmitida inalámbricamente vía Wifi utilizando un módulo de transmisión, como se esquematiza en la figura 15-1

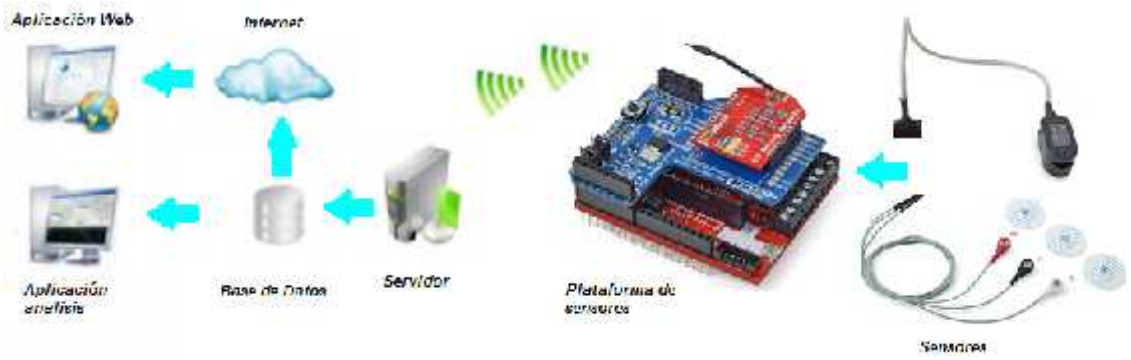


Figura 15-1: Esquema General del Sistema de Telemonitoreo

Realizado por: M. Ramírez y F. Jiménez, 2015

1.4 Seguridad de Red e Información

1.4.1 Fundamentos de Seguridad de Red e Información

Para que un sistema informático se comporte tal y como se espera de él, este sistema debe estar libre de todo peligro daño o riesgo, para ello es necesario la aplicación de aspectos que garanticen el diseño de seguridad Informática tales como: Confidencialidad, Integridad y Disponibilidad.

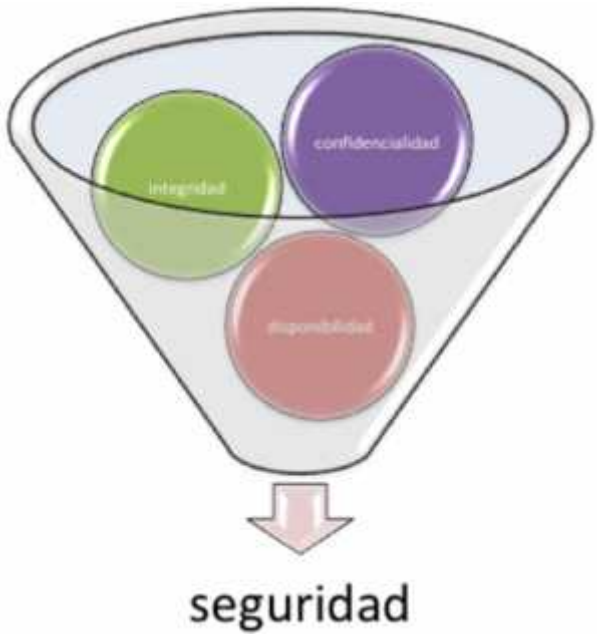


Figura 16-1: Conceptos Básicos de la Seguridad

Fuente: www.sistemasumma.com, 2010

1.4.1.1 Confidencialidad

Se entiende como confidencialidad al acceso único de usuarios autorizados vigilando de tal manera que estos no van a convertir esa información en disponible para otros.

Teniendo en cuenta que en la red existen dos tipos de datos; los datos grabados (saved) que se encuentran en dispositivos finales (Servidores, PCs, Tablets, etc) y los datos en movimiento (motion) que viajan a través de la red; debemos implementar mecanismos que aseguren ambas partes, es decir técnicas de cifrado o encriptación.

En la salud se considera que la información forma parte de la intimada de cada paciente por lo que se debe proteger y dar acceso únicamente al personal autorizado.

Los mecanismos para preservar la confidencialidad de información son:

- Control de acceso a los sistemas.

El control de acceso consiste en conceder permisos para acceder a datos y recursos de un sistema. Se basa principalmente en dos conceptos: identificación y autenticación.

Identificación es la acción de presentar su identidad a un sistema, generalmente usando un identificador de usuarios.

Autenticación es la confirmación de que un usuario que intenta acceder al sistema es válido. Para esta comprobación se pueden utilizar; contraseñas, características biométricas, algo que el usuario posee (tarjeta magnética) o algo que solo el usuario es capaz de hacer (patrones de escritura).

- Cifrado o encriptación de la información.

Es una de las técnicas más utilizadas para lograr un nivel de seguridad alto en un sistema. Consiste en alterar la información original con el fin de que no sea reconocible para cualquier persona. Existen dos tipos de cifrado: simétrico y asimétrico.

El simétrico corresponde al uso de una sola clave tanto para el cifrado como para el descifrado de la información, dicha clave la deben conocer tanto el emisor como el receptor. Aunque el uso de un cifrado simétrico garantiza los tres criterios de seguridad muchas veces el traspaso de la contraseña de descifrado es un inconveniente ya que si en algún punto es interceptada toda la información estaría vulnerable.

El cifrado asimétrico consiste en el uso de dos claves una pública conocida por todos y otra privada conocida únicamente por el receptor. La clave pública es utilizada para el cifrado y la privada para el descifrado de los datos. Pese a que se conservan los criterios principales de la seguridad este es un mecanismo más complejo y de mayores requerimientos computacionales por lo que su uso se realiza en combinación con técnicas simétricas, es decir, los datos se realizan con un cifrado simétrico y la clave es enviada con técnica asimétrica.

1.4.1.2 Integridad

Se refiere al tratamiento de la información, es decir que los datos transmitidos de un punto a otro no sean modificados bajo ningún concepto. Sin embargo, dependiendo del tipo de información solo pueden ser modificados por elementos autorizados, y de una manera controlada.

Para comprobar que la información no sea corrupta, se implementan algoritmos de hashing. Un hash es una función matemática que proporciona un resumen particular de la información original.

Una función hash debe cumplir con las siguientes propiedades:

- Generar un mensaje de tamaño fijo
- Fácil y rápido de calcular a partir del mensaje
- Dificultad al construir un mensaje para que resulte un determinado hash
- Dificultad para modificar un mensaje de manera que el hash se mantenga
- Dos mensajes diferentes no deben tener el mismo hash

1.4.1.3 Disponibilidad

La información y la red deben estar siempre disponibles en el momento oportuno. La disponibilidad de la red siempre se verá amenazada por ataques informáticos de distinta índole, principalmente por ataques de Denegación de servicio (DoS) o Denegación de servicio distribuido (DDoS).

Los ataques de Denegación de servicio (DoS), no violan la confidencialidad ni la integridad de la información, afectan directamente la disponibilidad, por lo que se deben tomar medidas especialmente para este tipo de ataques, además de contar con servidores redundantes, backups entre otras.

Cuando se habla de seguridad de red e información, nos referimos a una administración de riesgo; despejando incógnitas tales como: qué se protege y de quién se protege, para lo cual se requiere hacer un estudio de factibilidad.

1.4.1.4 Activos

Representa todo lo que tiene valor para una organización, sean estos tangibles (personas, equipos, dinero, etc) o intangibles (propiedad intelectual, base de datos, lista de contactos, etc)

1.4.1.5 Vulnerabilidad

La vulnerabilidad se refiere a una deficiencia o falla de seguridad que son susceptibles a ser atacadas en diferentes niveles que pueden ser: de red, protocolo, o Sistema Operativo. Las vulnerabilidades pueden ser explotadas (exploit), representando amenazas activas cuando el administrador por ignorancia o negligencia no toma las medidas necesarias para mitigar o reducir la misma; y pasivas (latente) cuando existe, pero nadie toma ventaja de ella.
Entre las vulnerabilidades que puede tener un sistema se encuentran:

- Políticas de Seguridad
- Errores de diseño
- Debilidades de protocolo
- Mal configuración
- Vulnerabilidades de software
- Factores Humanos
- Software maliciosos
- Vulnerabilidades de hardware
- Accesos Físicos

1.4.1.6 Amenazas

Es todo elemento o acción capaz de producir un daño (material o inmaterial) contra los recursos de un sistema. Entre las amenazas actuales que pueden atentar la seguridad de un sistema están:

- Terroristas
- Criminales
- Agencias del gobierno
- Estados/Nación
- Hackers
- Empleados disgustados
- Competencia
- Cualquiera con acceso a Internet

1.4.1.7 Riesgo

Es la probabilidad de sufrir un ataque por parte de alguna amenaza, por lo cual se debe realizar un análisis del riesgo y tomar decisiones para mejorar la protección del sistema.

1.4.1.8 Contramedida

Son medidas o acciones que se deben tomar para mitigar el riesgo en la red, aplicando las diferentes técnicas de seguridad.

1.4.2 Ataques

Cualquier acción inteligente y deliberada (especialmente en el sentido de método o técnica) para eludir los servicios de seguridad y violar la política de seguridad de un sistema.

1.4.2.1 Tipos de Ataques

A nivel de tecnología hay varios métodos de ataques, pero no existe un estándar para categorizarlos, en ese caso se pueden citar los siguientes:

- Ataques de Reconocimiento consisten en el descubrimiento y mapeo de sistemas, servicios o vulnerabilidades sin autorización, empleando aplicaciones y herramientas de sniffers de paquetes (wireshark) y escáneres de puertos (Nmap) en la red con el objetivo para determinar qué direcciones IP están siendo utilizadas y qué servicios o puertos están disponibles.

- Ingeniería Social se aprovecha de las vulnerabilidades personales engañando a un miembro de una organización para que le proporcione información valiosa, como la ubicación de los archivos o de las contraseñas. La suplantación de identidad es un tipo de ataque de ingeniería social que no requiere habilidad informática alguna ya que el atacante se hace pasar por una persona de confianza que tiene una necesidad aparentemente legítima de obtener información confidencial.

- Ataques de acceso es la capacidad de obtener privilegios utilizando varios métodos, incluyendo ataques de fuerza bruta, programas troyanos, puertas traseras (backdoors) falsificación de IPs y sniffers de paquetes para conseguir datos, contraseñas y para así ganar acceso. Los ataques de acceso en general pueden ser detectados revisando los registros en el log, el uso del ancho de banda y la carga de los procesos.

- Denegación de servicios (DoS), estos ataques intentan comprometer la disponibilidad de una red, un host o una aplicación y se los considera un riesgo importante porque pueden interrumpir fácilmente un proceso de negocios y causar pérdidas significativas saturando la red para que el tráfico de usuario válido no pueda pasar. Un ataque DoS se aprovecha del hecho de que los sistemas objetivos como los servidores deben mantener información por lo que explotan estos enviando tamaños de paquetes o valores de datos que no son esperados siendo incapaz de manejarlos haciendo que el sistema se vuelva lento y colapse. Existe en

similar intención un ataque DoS llamado Denegación de Servicio Distribuido (DDoS) éste se origina en múltiples fuentes coordinadas.

1.4.2.2 Mitigación de Ataques de Red

El tipo de ataque determina la manera de mitigar las amenazas en una red. Los ataques pueden ser mitigados de varias maneras: la autenticación con contraseñas robustas, la criptografía, software y herramientas anti sniffer, infraestructura switcheada, uso de IPS y Firewall en conjunto con políticas de seguridad pueden reducir el número de ocurrencias de amenazas como parte de defensa de un sistema englobado de mitigación, aunque esto no elimina completamente el riesgo de ataque lo disminuye en gran medida.

1.4.3 Análisis y Administración del Riesgo

Es un método para determinar, analizar, valorar y clasificar los posibles riesgos en el cual se establecen mecanismos que permitan controlarlos y mitigar las amenazas al sistema.

1.4.3.1 Ciclo de Vida de Seguridad de Red

Es un modelo conceptual que hace referencia al Modelo OSI en términos de seguridad.
Antes de implementar cualquier solución de seguridad en una red informática en general, debemos identificar los riesgos y amenazas y en lo posible etiquetarlos según su impacto; este procedimiento le llamamos iniciación o planeación. Luego de profundizar en los diferentes riesgos podemos analizar la adquisición y desarrollo del software, hardware, políticas y contramedidas necesarias que implementaremos para mitigar dichos riesgos y monitorear cualquier eventualidad.

Figura 17-1: Ciclo de vida de la Seguridad

Fuente: www.redysecurity.com, 2013

En la figura 17-1 se detalla el modelo de ciclo de vida de la seguridad, siendo sus fases; planeación, políticas de implementación, monitoreo y administración, detección de intrusos, evaluación de seguridad, análisis de riesgos y amenazas y creación de políticas de seguridad.

1.4.3.2 Método de Análisis de Riesgo

"El riesgo total es un conjunto de elementos que se conforman entre sí con la finalidad de calcular el posible impacto promedio en base a la probabilidad de ocurrencia de cada amenaza detectada durante el análisis realizado. El riesgo residual es el resto que queda luego de efectuar una mitigación a los riesgos existente" (Andrés Meneses y Sergio Parra, 2015, p 5).

Planteando una relación entre estos conceptos se establece la siguiente formula:

RT (Riesgo Total): Probabilidad x Impacto Promedio

1.4.4 Fundamentos de Firewall

1.4.4.1 Concepto

Llamado también cortafuegos es un sistema que permite proteger a la red de intrusos provenientes de una red exterior (internet). Un firewall puede ser un software, hardware o una combinación de ambos por el cual pasa todo el tráfico de datos tanto saliente como entrante y en el que se aplica un filtrado de paquetes tomando decisiones sobre permitir o denegar el paso de dichos paquetes. En la figura 18-1 se puede representar el funcionamiento de un firewall.

Figura 18-1: Firewall

Fuente: www.microsoft.com, 2014

1.4.4.2 Objetivo del Firewall

Debe ser un software, equipo o grupo de equipos resistente a ataques informáticos, ya que este es el punto crítico para prevenir que un tráfico malicioso tenga acceso a servidores y demás recursos de la red.

1.4.4.3 Tipos de Firewall

Un sistema firewall puede estar compuesto por muchos dispositivos y componentes diferentes, uno de ellos es el filtrado de tráfico. Hay varios tipos de firewalls de filtrado, entre ellos los siguientes:

- Firewall de filtrado de paquetes - (Packet-filtering firewall) Consiste en un router con la capacidad de filtrar paquetes con algún tipo de contenido establecidas en las reglas, como información de capa 3 y, en ocasiones, de capa 4.

- Firewall con estados - (Stateful firewall) Monitorea el estado de las conexiones, si están en estado de iniciación, transferencia de datos o terminación.

- Firewall gateway de aplicación (proxy) - (Application gateway firewall) Filtra según la información de las capas 3, 4, 5 y 7 del modelo de referencia OSI. La mayoría del control y filtrado del firewall se hace por software.

- Firewall de traducción de direcciones - (Address translation firewall) Expande el número de direcciones IP disponibles y oculta el diseño del direccionamiento de la red.

1.4.4.4 Limitaciones

Es importante saber que ningún sistema que se implemente brindará una absoluta seguridad, las amenazas siempre estarán presentes por lo cual se debe actualizar constantemente la seguridad implementada. Los firewalls ofrecerán protección en tanto las conexiones entrantes y salientes pasen obligatoriamente por este, además de utilizar los dispositivos específicos para esta finalidad y ser posible una correcta configuración.

Añadir medios de almacenamiento externos a los dispositivos de red es una violación a las políticas de seguridad general. Para aumentar la protección el firewall debe ejecutar un registro de actividad para controlar y poder detectar intentos de intrusión o anomalías.

Otro aspecto a tener en cuenta es la latencia o retardo que se genera en la rede debido a que todo el tráfico debe ser analizado por el firewall.

1.4.5 Fundamentos de Sistema Detección de Intrusos (IDS)/Sistema Prevención de Intrusos (IPS)

1.4.5.1 Diferencias entre IDS e IPS

Los sistemas de detección de intrusiones (Intrusion Detection Systems) o IDSs fueron implementados para monitorear de manera pasiva el tráfico de la red. Un IDS copia el tráfico de red y lo analiza en lugar de reenviar los paquetes reales. Compara el tráfico capturado con firmas maliciosas conocidas de manera offline del mismo modo que el software que busca virus. Esta implementación offline de IDS se conoce como modo promiscuo.

La ventaja de operar con una copia del tráfico es que el IDS no tiene efectos negativos sobre el flujo real de paquetes del tráfico reenviado. La desventaja de operar con una copia del tráfico es que el IDS no puede evitar que el tráfico malicioso de ataques de un solo paquete alcance el sistema objetivo antes de aplicar una respuesta para detener el ataque. El IDS generalmente requiere asistencia de otros dispositivos de red, como routers y firewalls, para responder a un ataque.

El sistema de prevención de intrusiones (Intrusion Prevention System) o IPS se apoya en la ya existente tecnología IDS. A diferencia del IDS, un dispositivo IPS se implementa en modo en línea. Esto significa que todo el tráfico de entrada y de salida debe fluir a través de él para ser procesado. El IPS no permite que los paquetes ingresen al lado confiable de la red sin ser analizados primero. Puede detectar y tratar inmediatamente un problema según corresponda.

El IPS monitorea el tráfico de capas 3 y 4 y analiza los contenidos y la carga de los paquetes en búsqueda de ataque sofisticados insertos en ellos, que pueden incluir datos maliciosos pertenecientes a las capas 2 a 7. Cuando un paquete pasa a través de una interfaz en un IPS, no es enviado a la interfaz de salida o confiable hasta haber sido analizado.

La ventaja de operar en modo en línea es que el IPS puede evitar que los ataques de un solo paquete alcancen el sistema objetivo. La desventaja es que un IPS mal configurado o una solución IPS inapropiada pueden tener efectos negativos en el flujo de paquetes del tráfico reenviado.

1.4.5.2 Terminología Positivo/Negativo

Cuando se trabajan con sistemas computacionales siempre se espera que la salida de la máquina sea el correcto, es decir que la información que la maquina emita sea verídica. Al implementar IPS/IDS aparecerán términos que debemos entender, como:

- Falso Positivo: Es un tráfico que existe en la red que no es malicioso pero que genera una alarma.

- Falso Negativo: Es cuando hay tráfico malicioso, pero no se genera una alerta, esto ocasionaría un problema de seguridad. Para prevenir este inconveniente se podría contar con una solución alterna que ayude con el control de tráfico; este puede ser un syslog. Este syslog serviría de bitácora para los sistemas, ya que en ella se registrará todo cuanto suceda y el administrador podrá verificar si existe o no anomalías.

- Positivo Verdadero: Este sería el caso idóneo de alertas, se da cuando existe un tráfico malicioso y se genera una alarma.

- Positivo Negativo: Corresponde al tráfico normal no malicioso, en ese caso no se genera ningún tipo de alerta.

1.4.5.3 Identificación de Tráfico Malicioso

Los sistemas de detección y prevención de intrusos utilizan los siguientes métodos para identificar el tráfico malicioso:

- Basado en Firmas o Reglas: Es cuando el IPS/IDS contiene una base de datos con reglas, el tráfico es analizado con cada una de estas reglas y de acuerdo actúa; permitiendo o rechazando el paquete.

- Basado en Políticas: Se definen políticas dentro del IPS/IDS. Son procedimientos que se crean de acuerdo al tipo de tráfico que se vaya a tener.

- Basado en Anomalías: Es un método automático basado en base line, este método es usado para analizar un promedio base que usualmente tiene la red. Si en algún momento el IDS/IPS analizan un tráfico y existe demasiada diferencia con el tráfico promedio se generaría una alerta.

- Basado en Reputación: Es un método de correlación, es decir que el IPS/IDS utiliza una base de datos global externa para analizar la reputación de tráfico.

1.4.6 Políticas de Seguridad

1.4.6.1 Definición

Según la RFC 2196[1](1997, p 6) "Una política de seguridad es una declaración formal de las reglas a las cuales se debe adherir el personal que tiene acceso a los bienes tecnológicos y de información de una organización".

Una política de seguridad es un documento dinámico, es decir se trata de un documento que nunca está terminado y que se actualiza constantemente de acuerdo a los cambios que existan tanto en tecnología como es personal.

1.4.6.2 Objetivos de una Política de Seguridad

Una política de seguridad debe cumplir los siguientes objetivos:

- Informar a los usuarios, al personal y a los directivos de la empresa acerca de los requisitos obligatorios para proteger los bienes de tecnología e información.

- Especificar los mecanismos a través de los cuales se pueden cumplir estos requisitos.

- Proporcionar una línea de base a partir de la que se pueda adquirir, configurar y auditar redes y sistemas informáticos para que cumplan la política.

1.4.6.3 Tipos de Políticas de Seguridad

Por su amplitud de cobertura e impacto, generalmente es un documento complejo que está diseñado para gobernar temas como acceso a los datos, navegación en la web, uso de las contraseñas, criptografía y adjuntos de correo electrónico. Entonces pueden existir:

- Políticas de email

[1] **RFC 2196.-** Es un manual de seguridad que puede ser usado como estándar para establecer Políticas de Seguridad

- Políticas de acceso remoto
- Políticas de telefonía
- Política para las aplicaciones
- Políticas para el uso de la red

1.4.6.4 Consideraciones para desarrollar una Política de Seguridad

Algunas instituciones proporcionan pautas para la elaboración de políticas de seguridad. No todas las organizaciones requieren aplicar la totalidad de los componentes que se mencionaran a continuación, dependerá de la actividad de cada empresa.

- Declaración de autoridad y alcance: define qué persona dentro de la organización propone la política de seguridad, quién es responsable de implementarla y qué áreas están contempladas por la política.

- Política de uso aceptable (AUP): define el uso aceptable de los servicios informáticos y las medidas de seguridad de los empleados adecuadas para proteger los recursos corporativos y la información confidencial de la organización.

- Política de identificación y autenticación: define qué tecnologías usa la empresa para garantizar que sólo el personal autorizado obtenga acceso a sus datos.

- Política de acceso a Internet: define qué es lo que la empresa permite y que no con respecto al uso de su conectividad a Internet por parte de empleados e invitados.

- Política de acceso al campus: define el uso aceptable de los recursos tecnológicos del campus por parte de los empleados y de los invitados.

- Política de acceso remoto: define la forma en la que los usuarios remotos pueden utilizar la infraestructura de acceso remoto de la empresa.

- Procedimiento para el manejo de incidentes: especifica quién responde ante incidentes de seguridad y cómo se deben manejar

- Política de solicitud de acceso a las cuentas: formaliza el proceso de solicitud de cuentas y de acceso dentro de la organización.

- Política de evaluación de adquisiciones: define las responsabilidades respecto de las adquisiciones de la empresa y los requisitos mínimos de las evaluaciones de adquisiciones que el grupo de seguridad de la información debe llevar a cabo.

- Política de auditoría: define las políticas de auditoría para garantizar la integridad de la información y de los recursos. Incluye un proceso para investigar incidentes, garantizar el cumplimiento de las políticas de seguridad y controlar la actividad de los usuarios y del sistema donde corresponda.

- Política de confidencialidad de la información: define los requisitos necesarios para clasificar y asegurar la información de la manera correspondiente en cuanto a su nivel de confidencialidad.

- Política de contraseñas: define las normas para crear, proteger y modificar contraseñas sólidas.

- Política de evaluación de riesgos: define los requisitos y otorga la facultad al equipo de seguridad de la información a identificar, evaluar y subsanar riesgos de la infraestructura de la información asociados con la conducción de los negocios.

- Política global de servidores Web: define las normas exigidas por todos los hosts Web.

- Política de acceso telefónico: define el acceso telefónico adecuado y su uso por personal autorizado.

- Política de acceso remoto: define las normas para conectarse a la red de la organización desde cualquier host o red externos a la organización.

- Política de seguridad de las VPN: define los requisitos de las conexiones de las VPN a la red de la organización.

1.5 Sophos

Es un software de seguridad para el punto final de comunicación, el cifrado, seguridad de red, seguridad de correo electrónico y la seguridad móvil, así como la gestión unificada de amenazas. Entre sus principales módulos de protección se encuentran:

- Protección de redes
- Protección de redes inalámbricas
- Protección web
- Protección de estaciones de trabajo
- Protección de correo electrónico
- Protección de servidores web

Los requerimientos de hardware para la instalación de Sophos UTM son los siguientes:

- Disco Duro: Mínimo 20 Gb en discos IDE, SCSI o S-ATA.
- Procesador: Dual Core de al menos 2.0 Ghz.
- Memoria RAM: Mínimo 1024 MB - Mínimo 2 tarjetas de red.

1.6 Políticas de Seguridad del Sistema de Telemonitoreo Médico

1.6.1 Disposiciones Generales

1.6.1.1 Alcance

Esta guía de políticas de seguridad es elaborada de acuerdo a los riesgos y vulnerabilidades encontradas en un sistema de telemonitoreo médico en pacientes ambulatorios y no ambulatorios usando sensores no invasivos. Esta política es aplicable a todo el personal médico, paciente y cualquier individuo externo que tenga relación con el tratamiento de la información obtenida.

1.6.1.2 Objetivos

Proporcionar una guía de las normas y procedimientos que los pacientes y personal médico deben cumplir para la protección de hardware, software e información del sistema de telemonitoreo.
Planear, organizar, dirigir y controlar las actividades para mantener y garantizar un riesgo de amenazas mínimo a los recursos informáticos manteniendo así la integridad, confidencialidad y disponibilidad de la información de pacientes.

1.6.1.3 Responsable

El personal médico administrativo será el responsable de vigilar y controlar la correcta aplicación de las políticas de seguridad con el fin de proteger los activos informáticos, así como la información procesada en ellos.

1.6.1.4 Evaluación de las Políticas

Las políticas tendrán una revisión semestral para realizar actualizaciones, modificaciones y ajustes basados en el análisis de nuevos riesgos, amenazas y cambios en la infraestructura.

1.6.2 Lineamientos para la adquisición de dispositivos y software

1.6.2.1 Desarrollo Tecnológico

En la adquisición de dispositivos para el telemonitoreo se deberá considerar el avance tecnológico del momento, es decir se podrán adquirir nuevo equipamiento siempre cuando mejore la calidad de atención al paciente.

1.6.2.2 Estándares

Todo sensor médico adquirido debe estar homologado por la Agencias de regulación de cuidados de la salud para el telemonitoreo de pacientes.

1.6.3 Seguridad Física

1.6.3.1 Protección Física de Servidores y Sensores

Todos los sistemas informáticos en especial los servidores deben estar en un lugar limpio, libre de humedad y protegidos de cualquier acceso no permitido.

Deberá recibir limpieza al menos una vez cada 15 días para mantenerlo libre de polvo y esta acción deberá ser realizada por el encargado de mantenimiento informático previa autorización. Además de revisar conexiones eléctricas para garantizar la funcionalidad del sistema.

Los sensores biomédicos utilizados deben ser evaluados periódicamente para comprobar su correcta funcionalidad, es decir revisar que los datos que están transmitiendo son correctos y por

alguna u otra razón no son alterados. Además, el paciente debe comprometerse a realizar un buen uso de estos y no maniobrar de tal manera que el dispositivo quede defectuoso.

Tanto el personal médico como los pacientes deben salvaguardar la integridad de los dispositivos, por lo tanto, deben informar de cualquier daño o avería que tengan estos y más aún si contienen información importante.

1.6.3.2 Respaldos

Los registros de datos obtenidos desde los sensores serán respaldados periódicamente automática y manualmente, y almacenados en lugares seguros teniendo acceso restringido a personas no autorizadas.

1.6.4 Seguridad Lógica

1.6.4.1 Manejo de Servidores

El acceso al servidor es restringido, únicamente la persona encargada de su mantenimiento podrá acceder, sin embargo, deberá tener autorización para hacerlo y un respectivo registro.

La información de los servidores deberá respaldarse de acuerdo a su nivel de importancia, puede ser diaria, semanal o mensualmente.

1.6.4.2 Correos Electrónicos

El personal médico tiene prohibido acceder a correos electrónicos externos o personales.

En caso de usar el correo para envió de información confidencial, debe ir encriptado y destinado exclusivamente a personas autorizadas y si así lo permite sus funciones y responsabilidades.

Queda prohibido tratar de falsificar, suplantar o sustituir la identidad de un correo electrónico.

1.6.4.3 Datos de Pacientes

El acceso a datos críticos de pacientes será permitido al personal médico autorizado, o al paciente en caso de tratarse de un control rutinario.

1.6.4.4 Identificación de Usuarios y Contraseñas

Toda persona que tenga acceso al sistema debe disponer de una única autorización de usuario y contraseña, luego de haber aceptado las políticas de seguridad.

Cada usuario recibirá una contraseña aleatoria la misma que puede ser cambiada posteriormente considerando los procedimientos de establecer una contraseña segura, es decir combinación de números, letras y signos especiales en una longitud no menor a 8 caracteres.
Tanto pacientes y personal médico tendrán acceso autorizado exclusivamente a aquellos datos y recursos que se precisen para el desarrollo de sus funciones o de manera informativa en el caso de pacientes.

Los identificadores de usuarios se establecen por un periodo de tiempo, una vez expirado se renovarán y si el usuario ya no existe se desactivarán.

1.6.5 Seguridad de Infraestructura

1.6.5.1 Firewall

Desactivar el firewall del sistema operativo y aplicar reglas de seguridad generalizadas utilizando un software o equipo robusto que englobe todo el sistema, es decir que controle el tráfico que ingrese o salga ya sea de pacientes o servidores.

1.6.5.2 Conectividad a Internet

La conexión a Internet debe ser única y exclusivamente para actividades que correspondan con las funciones laborales.

Su acceso debe ser establecido a través del sistema de seguridad de firewall.

No se permite acceder directamente a proveedores de servicios utilizando otros medios de conexión (modem).

1.6.5.3 Uso de dispositivos extraíbles

Para el uso de dispositivos de almacenamiento externo se deberá tener una autorización por parte de los responsables de cuidar la seguridad de los datos además de justificar su uso.

El portador de este tipo de dispositivos será responsable de un buen uso y responderá por la confidencialidad e integridad de la información que este contenga.

1.6.6 Plan de Contingencia

En caso de interrupciones de trabajo del servidor principal por cualquier motivo debe entrar en funcionamiento el servidor de respaldo para continuar con su normal funcionamiento.

Los respaldos deben estar en lugares seguros fuera del alcance de gente mal intencionado y no cerca de los mismos equipos.

Contar con un instructivo correctivo de fallas para tratar de reconstruir la mayor parte de información.

Tener un directorio de personal técnico informático en caso de requerirlo.

Ejecutar las respectivas pruebas de funcionalidad del plan.

Mantener actualizadas las políticas considerando los avances tecnológicos y posteriores amenazas informáticas que se puedan originar.

CAPÍTULO II

2. MARCO METODOLÓGICO

2.1 Diseño de la Investigación

En el desarrollo de este proyecto se establecieron tres fases para alcanzar los objetivos propuestos. Fase de análisis general, fase de desarrollo del proyecto, y pruebas de implementación.

Fase de análisis general
En esta fase se estudiará el estado actual de la atención hospitalaria a personas geográficamente distantes y las ventajas que le proporcionaría una atención de calidad y oportuna utilizando las tecnologías en boga. Además, se analizará la importancia que tiene la implementación de medidas de seguridad de la información en toda empresa.

Fase de desarrollo del proyecto
Esta fase servirá para recopilar aspectos sobre un sistema de seguridad de la información basado en la norma ISO 27001[2], considerando la importancia de salvaguardar los cimientos principales de la seguridad; confidencialidad, integridad y disponibilidad. Por otro lado, se examinará la manera de implementar un ambiente de prueba adquiriendo los materiales necesario para ese fin, y simulando el monitoreo de un individuo a un sistema que previamente se abran implementado medidas de seguridad informática.

Fase de pruebas de implementación
Una vez se halla implementado el ambiente de prueba para el telemonitoreo es necesario comprobar que las reglas de seguridad efectuada en Sophos se han realizado con éxito.

2.2 Tipo de Investigación

La presente investigación es de tipo descriptiva-aplicada debido a que el propósito es dar solución ante un problema aplicando conocimientos y estableciendo estrategias o una guía de

[2] ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

proceder que garantice la atención eficaz y oportuna a un individuo y además certifique la seguridad de la información.

2.3 Métodos

Los métodos empleados para el desarrollo de este proyecto son: documental o teórico y de campo.

El método documental se aplicará al momento de la recolección de información en cual acudiremos a trabajos, libros, tesis, blog, paper y demás fuentes de información realizadas o editadas por otros autores, esto con el fin de profundizar conocimientos y llegar a cumplir los objetivos propuestos.

El método de campo lo aplicaremos una vez planteado nuestro marco teórico y habiendo investigado la información necesaria, implementaremos un ambiente de prueba con el fin de comprobar la robustez de nuestro sistema de seguridad.

2.4 Técnicas

Las técnicas a utilizar son:

- Observación
- Recopilación teórica
- Análisis de contenido
- Pruebas sobre la implementación

2.5 Fuentes de Información

Toda fuente de información será revisada y analizada, entre se pueden citar las siguientes:

- Tesis digitales
- Blog
- Revistas electrónicas
- Artículos científicos
- Sitios y páginas web

2.6 Recursos

2.6.1 Recursos Humanos

Dentro de la parte humana intervienen:

- Autores de tesis
- Director de tesis
- Miembros
- Voluntario para mediciones de señal

2.6.2 Recursos Materiales

Hojas de papel bond

Estante para ambiente de prueba

Flash Memory

CD´s

2.6.3 Recursos Técnicos y Tecnológicos

Tabla 1-2: Descripción de Recursos Técnicos y Tecnológicos

RECURSOS	DECRIPCIÓN
Computadora de Escritorio	En ella se instalará Sophos, programa que nos servirá de firewall y aplicar las reglas de seguridad.
Laptop	Se estipula su funcionamiento para ser el servidor del sistema.
Plataforma de sensores e-health	Dispositivo especializado en el trabajo experimental de telemonitoreo, servirá para conectar los sensores que leerán las señales del cuerpo.
Módulo Arduino Uno	En él se conectará la plataforma de sensores, y servirá de puente de comunicación ya que se programará para que realice las funciones requeridas.
Módulo Wifi 232-b	Terminal que establecerá la comunicación inalámbrica entre el servidor y los sensores.
Sensor biomédico Pulsioximetro	Dispositivo que se coloca en el dedo para determinar señales de pulso y porcentaje de oxígeno en la sangre.
Sensor biomédico Electrocardiograma	Dispositivo utilizado para detectar las señales ECG.
Dispositivo móvil	Cualquier terminal móvil que se pueda conectar a l servidor remoto.

Tarjeta Ethernet	Es necesaria una tarjeta de red adicional que se implementará en la computadora de escritorio, ya que un firewall requiere de dos interfaces.
Punto de Acceso	Dispositivo que funcionará como punto de acceso inalámbrico en el ambiente de prueba
Impresora	Necesaria para la impresión de la documentación
Internet	Útil durante el tiempo de investigación del marco teórico.
Sophos	Software que se implementará como firewall del sistema

Realizado por: M. Ramírez y F. Jiménez, 2015

2.7 Planteamiento de la Hipótesis

"La Implementación de un sistema de gestión de seguridad garantizará la confidencialidad, integridad y disponibilidad de la información en el Prototipo de Telemonitoreo Médico."

2.8 Población y Muestra

2.8.1 Población

Para el presente trabajo se aplicará la definición de población diana ya que se desarrollara a partir de los objetivos de estudio.

Son múltiples los sistemas de monitoreo médico implementados a efecto de controlar y mejorar la salud de pacientes especialmente con problemas coronarios, cardíacos, respiratorios que miden las diferentes funciones de los órganos del cuerpo humano a efecto de lograr a través de internet y el uso de múltiples tecnologías inalámbricas prestar la atención oportuna procurando el mejoramiento de la salud del paciente. Además de considerar varios sistemas para la gestión de Seguridad que prestar una gran variedad de funcionalidades.

2.8.2 Muestra

Para la determinación de la muestra se aplicará el muestreo aleatorio simple al realizar una selección al azar del software y hardware utilizado para el sistema.

A través del uso de plataformas electrónicas y tecnología inalámbrica Wi-Fi se diseñará el Telemonitoreo de signos vitales. Por otro lado para la gestión de seguridad se recurrirá al sistema Sophos; éste a más de ser un agente ligero, fácil de implementar y fácil de administrar proporciona funciones de seguridad completa tanto para red como para la información.

2.9 Instrumentos de Recolección de Datos

Los instrumentos para la recolección de datos son sensores biomédicos eficaces al momento de tomar señales de ECG, pulso y porcentaje de oxígeno en la sangre de personas al azar transmitiendo dichos datos inalámbricamente hasta el servidor. Estos son signos vitales que siempre son controlados para evitar una alteración respiratoria además de un control del ritmo cardiaco, por lo que los proveedores de suministros de salud dan las facilidades necesarias para adquirirlos.

La plataforma ehealth configurada sobre Arduino Uno es esencial debido a su interfaz de configuración y su propósito de experimentación en telemonitoreo, además permite realizar pruebas previas de transmisión.

CAPÍTULO III

3. MARCO DE RESULTADOS

3.1 Gestión y análisis de Riesgo

Es una aproximación metódica en la que se realizará una valoración del riesgo con los siguientes pasos: determinación y categorización de activos, determinación de amenazas, estimación del impacto y del riesgo.

3.1.1 Determinación y Categorización de activos

Los activos detallados a continuación son basados en el sistema que se implementará:

Tabla 1-3: Categorización de Activos

CATEGORIZACIÓN DE ACTIVOS			
Tipo	**Código**	**Categoría**	**Ejemplo**
Activos de Información	I1	Información Electrónica	Bases de datos y otros documentos creados y/o conservados en medios electrónicos.
	I2	Información Escrita	Información y/o creada en papel
Activos de Software	S1	Software base o sistema operativo	Software Base o Sistema Operativo Windows, Linux, Unix, etc
	S2	Software o herramientas comerciales, utilitarios	Office, Adobe, etc
	S3	Software desarrollado por terceros	Oracle, Sophos, etc
	S4	Software desarrollado internamente	Manuales, Guías, Políticas, etc
Activos de Hardware	H1	Equipos de procesamiento	Servidores, computadoras, laptops, sensores, etc
	H2	Equipo de comunicaciones	Routers, Switches, modulo inalámbrico, etc
	H3	Medios de Almacenamiento	Discos portátiles, CD's, memoria USB, etc
Servicios	SG1	Servicios Generales	Energía eléctrica, Internet, etc

Realizado por: M. Ramírez y F. Jiménez, 2015

Para determinar las escalas aplicadas en las siguientes tablas se manejará instrumentos que permiten analizar cuantitativamente la percepción de los niveles utilizando para ello diferentes tipos de escalas de evaluación basados en un estándar de la *"Escala Likert"*

Tabla 2-3: Valoración de Activos

VALORACIÓN DE ACTIVOS	
Alto	Cuando la destrucción, modificación, propagación o interrupción de la información afecta seriamente la operatividad o imagen de la empresa.
Medio	Cuando la destrucción, modificación, propagación o interrupción de la información afecta considerablemente la operatividad de la empresa.
Bajo	Cuando la destrucción, modificación, propagación o interrupción de la información no afecta la operatividad o imagen de la empresa.

Realizado por: M. Ramírez y F. Jiménez, 2015

3.1.2 Clasificación de amenazas, probabilidad de ocurrencia e impacto

A continuación se detallan las amenazas que pueden atentar contra los activos del sistema.

Tabla 3-3: Clasificación de Amenazas

CLASIFICACIÓN DE AMENAZAS	
Amenazas	**Ejemplo**
Naturales	Inundaciones, sismos, Incendios, etc.
Humanas	Renuncias, huelgas, accidentes, etc.
Tecnológicas	Virus, hacking, red, fallas de software y hardware
Sociales	Protestas, vandalismo, violencia, etc.
Infraestructura	Energía, explosión, fuego, fallas, etc.

Realizado por: M. Ramírez y F. Jiménez, 2015

De igual manera se define la probabilidad de ocurrencia de una amenaza, en el cual se especifica una escala de 1(Muy bajo) hasta 5(Muy alto) de que ocurra tal o cual amenaza.

Tabla 4-3: Probabilidad de ocurrencia de amenazas

Valoración	Ocurrencia
5. Muy Alto	Casi seguro
4. Alto	Muy probable
3. Medio	Probable
2. Bajo	Relativamente improbable
1. Muy Bajo	Muy Improbable

Realizado por: M. Ramírez y F. Jiménez, 2015

Asimismo, se realiza la valoración del impacto que tendría al efectuarse una amenaza. Se mantiene la escala de 1(muy bajo) hasta 5(muy alto).

Tabla 5-3: Valoración de Impacto

Valoración	Impacto
5	Muy Alto
4	Alto
3	Medio
2	Bajo
1	Muy Bajo

Realizado por: M. Ramírez y F. Jiménez, 2015

3.1.3 Determinación del nivel de tolerancia de riesgos

Los riesgos expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la probabilidad de que amenazas y vulnerabilidades causen un incidente. El riesgo crece con el impacto y con la frecuencia de ocurrencia.

Como el riesgo nunca es eliminado solo mitigado se establecerá una escala de tolerancia de riesgo dada por:

Tabla 6-3: Nivel de Tolerancia de riesgos por impacto

Muy Alto	Mayor a 40
Alto	30 a 40
Moderado	21 a 30
Bajo	10 -20
Muy Bajo	Menor a 10

Realizado por: M. Ramírez y F. Jiménez, 2015

En la siguiente tabla se detallan en análisis de riesgos:

Tabla 7-3: Análisis de riesgos del sistema

Código	Descripción	Probabilidad de Ocurrencia	Objetivo Afectado	Valoración de Impacto	Nivel de Tolerancia
R1	Manipulación indebida de la información	4	Tiempo	3	Bajo
			Costo	4	
			Servicio	4	
R2	Manipulación incorrecta de dispositivos de telemonitoreo	5	Tiempo	4	Moderado
			Costo	4	
			Servicio	4	
R3	Administración incorrecta de las reglas de seguridad	1	Tiempo	4	Muy Bajo
			Costo	5	
			Servicio	5	
R4	Acceso al sistema de personas no autorizadas	4	Tiempo	4	Bajo
			Costo	3	
			Servicio	4	
R5	Falla del sistema por software malicioso	4	Tiempo	2	Alto
			Costo	1	
			Servicio	2	
R6	Fallas de equipos de comunicación	2	Tiempo	3	Moderado
			Costo	3	
			Servicio	4	
R7	Fallas eléctricas	3	Tiempo	2	Alto
			Costo	1	
			Servicio	4	
R8	Daño de quipos por aspectos ambientales	1	Tiempo	4	Muy Alto
			Costo	4	
			Servicio	5	
R9	Incumplimiento de las políticas de seguridad	2	Tiempo	5	Muy Bajo
			Costo	5	
			Servicio	5	

Realizado por: M. Ramírez y F. Jiménez, 2015

3.2 Análisis de Cumplimiento de requerimientos de seguridad

Tabla 8-3: Análisis de cumplimiento de requisitos de seguridad

Ítem	Requisito	Cumple	Porcentaje de Cumplimiento	
Generalidades				**Promedio**
1	Definición de una Políticas de Seguridad	SI	75%	38%
2	Gestión y análisis de Riesgos	SI	80%	
3	Mantenimiento de registros	SI	50%	
4	Implementación de la Política de Seguridad	SI	50%	
5	Monitoreo de la implementación de controles	SI	60%	
6	Método para la capacitación del personal	NO	0%	
7	Método para la evaluación de incidentes	NO	0%	
Seguridad Lógica				
8	Definición y administración de usuarios	SI	70%	66%
9	Control de los derechos asignados a usuarios	SI	50%	
10	Controles sobre utilidades del sistema	SI	50%	
11	Controles de acceso al sistema	SI	80%	
12	Controles sobre acceso remoto	SI	80%	
Seguridad Personal				
13	Definición de responsabilidades sobre la información	SI	40%	43%
14	Procedimiento en caso de incumplimiento de las políticas de seguridad	SI	30%	
15	Procedimiento en caso de revocaciones de derechos de usuario	SI	60%	
Seguridad Física y Ambiental				
16	Daño o interferencia a la información	SI	65%	33%
17	Controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales	NO	0%	
Categorización de Activos y Clasificación de la Información				
18	Realizar y mantener un inventario de los activos	SI	100%	100%
19	Realizar una clasificación de la información, que debe indicar el nivel de riesgo existente	SI	100%	
Administración de las Comunicaciones				
20	Documentación para la operación de los sistemas	Si	5%	52%
21	Control sobre los cambios en el ambiente operativo, que incluye cambios en los sistemas de información, las instalaciones de procesamiento y los procedimientos	NO	0%	

22	Separación de funciones para reducir el riesgo	SI	40%	
23	Separación de los ambientes de desarrollo y pruebas	SI	60%	
24	Monitoreo del servicio dado por terceras partes	NO	0%	
25	Controles preventivos y de detección sobre el uso de software de procedencia dudosa, virus y otros similares	SI	80%	
26	Seguridad sobre las redes, medios de almacenamiento y documentación de sistemas	SI	100%	
27	Seguridad en transmisión de la información	SI	95%	
28	Seguridad sobre canales electrónicos	SI	40%	
29	Monitoreo del uso de los sistemas	SI	100%	
Adquisición y mantenimiento de sistemas informáticos				
30	Análisis de nuevos sistemas o mejoras en sistemas	SI	20%	73%
31	Aplicar técnicas de encriptación	SI	100%	
32	Controlar vulnerabilidades existentes en los sistemas	SI	100%	
Procedimientos de Respaldo				
33	Procedimiento de respaldo periódico	SI	50%	75%
34	Conservar los respaldos en lugares distantes	SI	100%	
Gestión de incidentes de seguridad de la información				
35	Procedimientos para el reporte de incidentes de seguridad de la información y las vulnerabilidades asociadas con los sistemas de información	SI	100%	85%
36	Procedimientos establecidos para dar una respuesta adecuada a los incidentes y vulnerabilidades de seguridad reportadas	SI	70%	

Realizado por: M. Ramírez y F. Jiménez, 2015

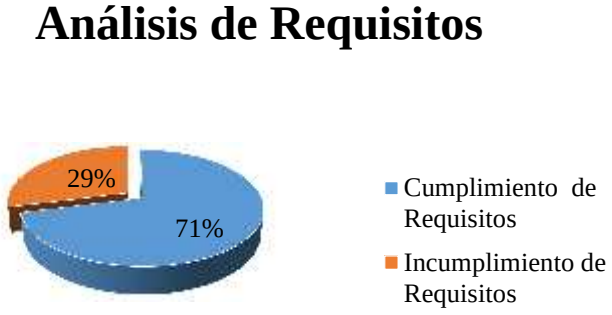
En la tabla 8-3 se realizó un análisis de los requisitos del sistema especificando el porcentaje de cumplimiento del mismo.

Tabla 9-3: Promedio de Cumplimiento de requisitos

Requisitos	1	2	3	4	5	6	7	8	9	**Promedio**
Cumplimiento de Requisitos	63%	66%	43%	65%	100%	65%	73%	75%	85%	71%
Incumplimiento de Requisitos	37%	34%	57%	35%	0%	35%	27%	25%	15%	29%

Realizado por: M. Ramírez y F. Jiménez, 2015

En el siguiente gráfico se representa la diferencia promedio del cumplimiento e incumplimiento de los requerimientos del sistema de seguridad



Gráfica 1-3: Análisis de cumplimiento de requisitos

Realizado por: M. Ramírez y F. Jiménez, 2015

3.3 Telemonitoreo

Para realizar el telemonitoreo se usan los sensores ECG y Pulsioxímetro, los mismos que están conectados a una plataforma de sensores ehealth configurada sobre una placa arduino UNO. Para la transmisión inalámbrica se usa un módulo wifi configurado según se muestra en el anexo A de este documento; en él se especifica además la dirección IP del dispositivo y la dirección del servidor al cual se transmitirán los datos.

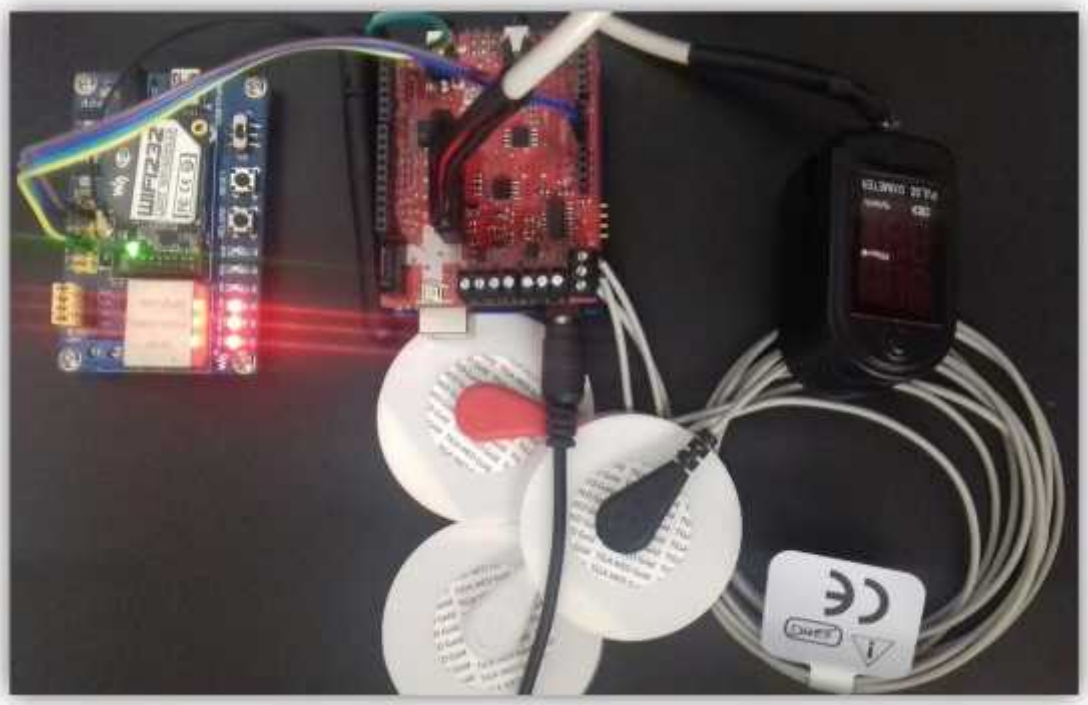


Figura 1-3: Telemonitoreo médico

Realizado por: M. Ramírez y F. Jiménez, 2015

Los datos configurados para el telemonitoreo son detallados en la siguiente tabla:

Tabla 10-3: Datos para Telemonitoreo

Dirección IP Servidor	10.10.10.10
Dirección IP Módulo Wifi	192.168.0.3
Protocolo en Servidor	TCP Server
Protocolo en Módulo Wifi	TCP Client
Puerto Local	8899

Realizado por: M. Ramírez y F. Jiménez, 2015

Monitoreo de Pulso y porcentaje de oxígeno en la sangre

Figura 2-3: Telemonitoreo Pulsioxímetro

Realizado por: M. Ramírez y F. Jiménez, 2015

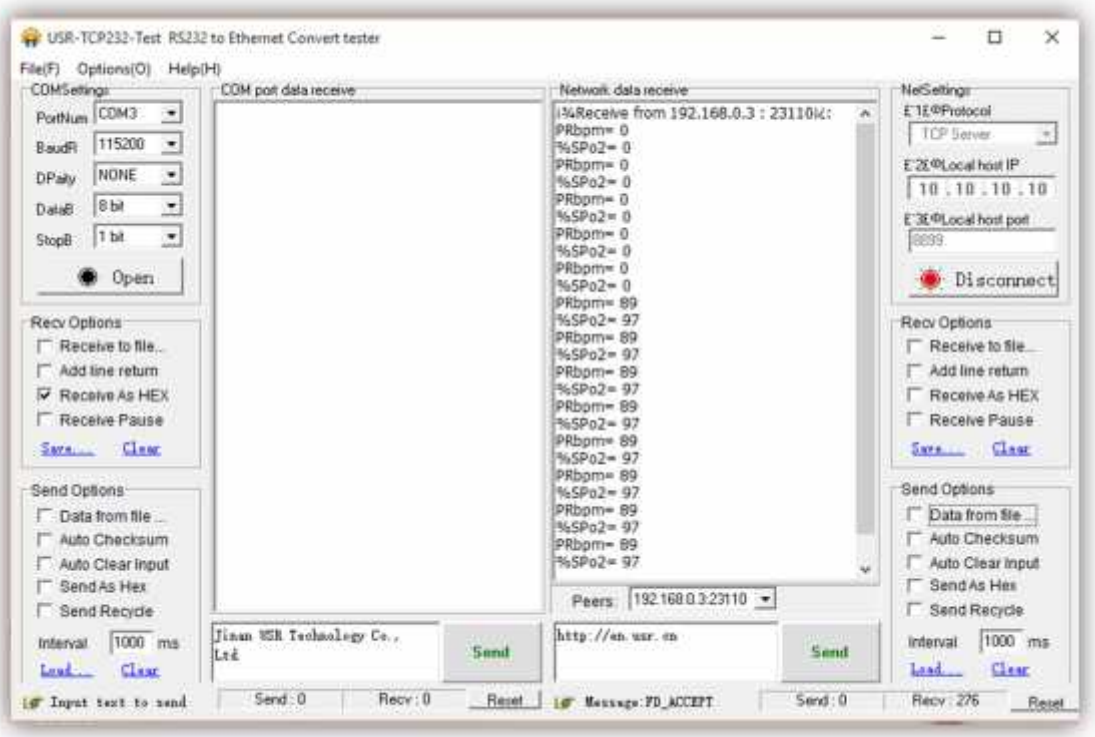


Figura 3-3: Recibiendo datos Pulsioxímetro

Realizado por: M. Ramírez y F. Jiménez, 2015

Monitoreo de ECG enviando la letra “B”

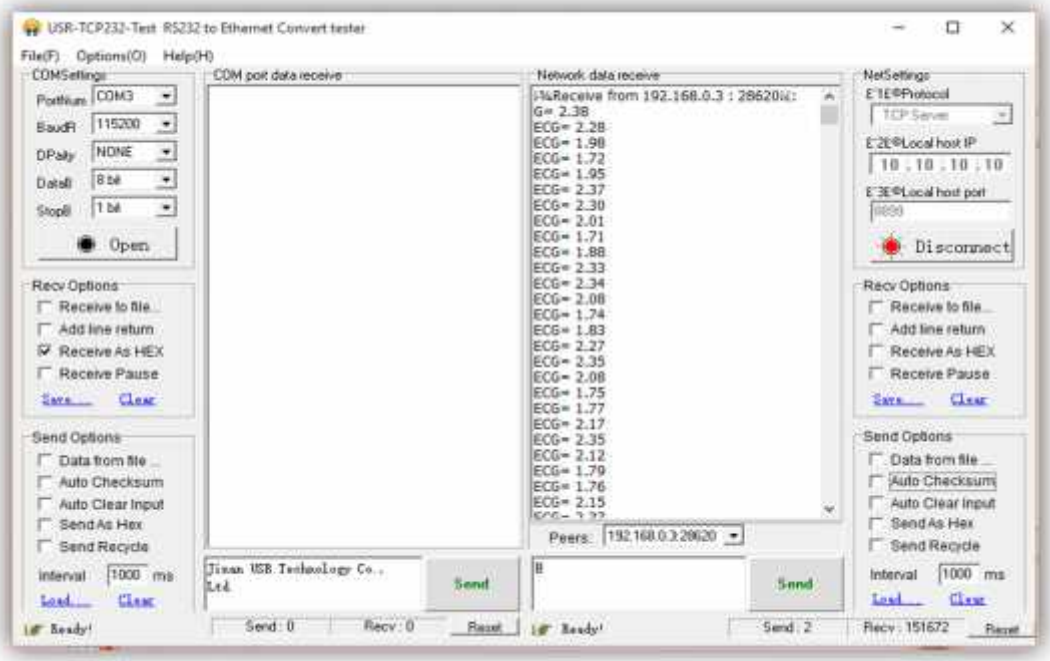


Figura 4-3: Recibiendo datos ECG

Realizado por: M. Ramírez y F. Jiménez, 2015

Monitoreo simultáneo del Pulsioxímetro y ECG enviando la letra “C”

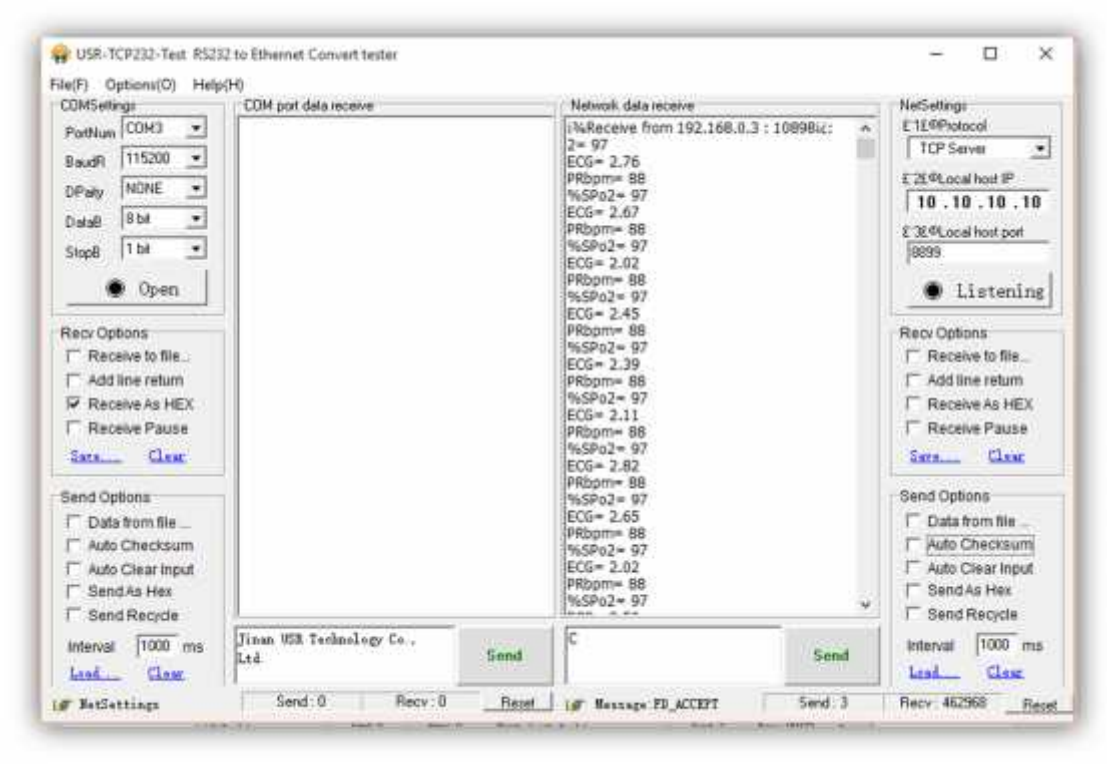


Figura 5-3: Recibiendo datos de telemonitoreo simultáneamente

Realizado por: M. Ramírez y F. Jiménez, 2015

Las siguientes imágenes muestran la interpretación de las señales ECG transmitidas en tiempo real en el software KST. Este software utiliza un archivo txt generado al recibir los datos en el servidor.

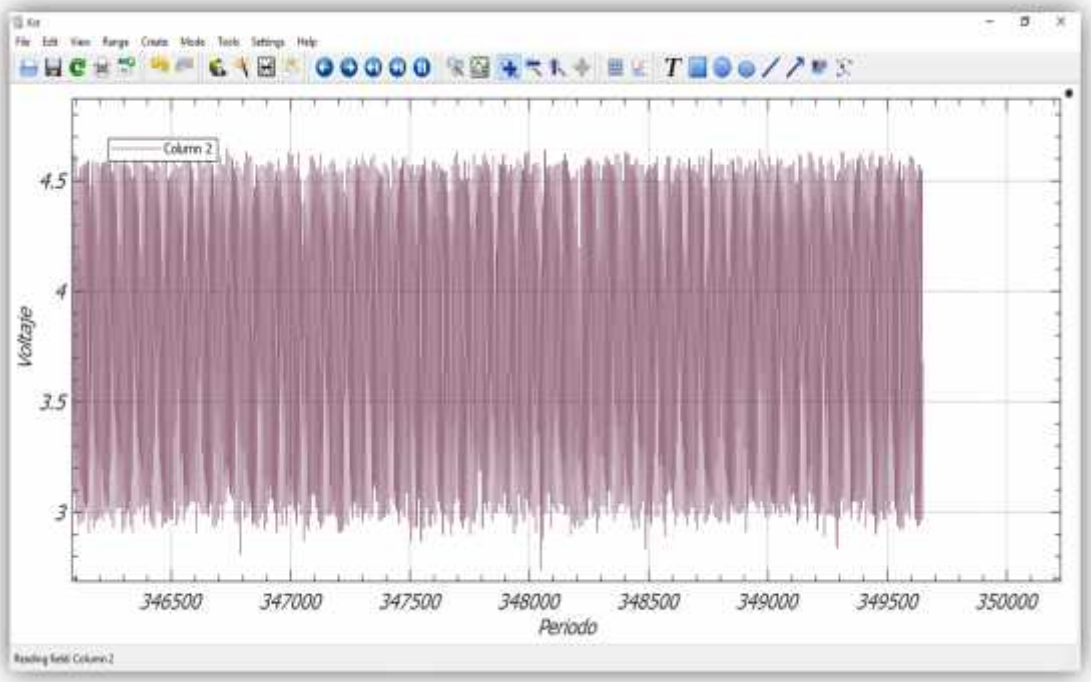


Figura 6-3: ECG 1

Realizado por: M. Ramírez y F. Jiménez, 2015

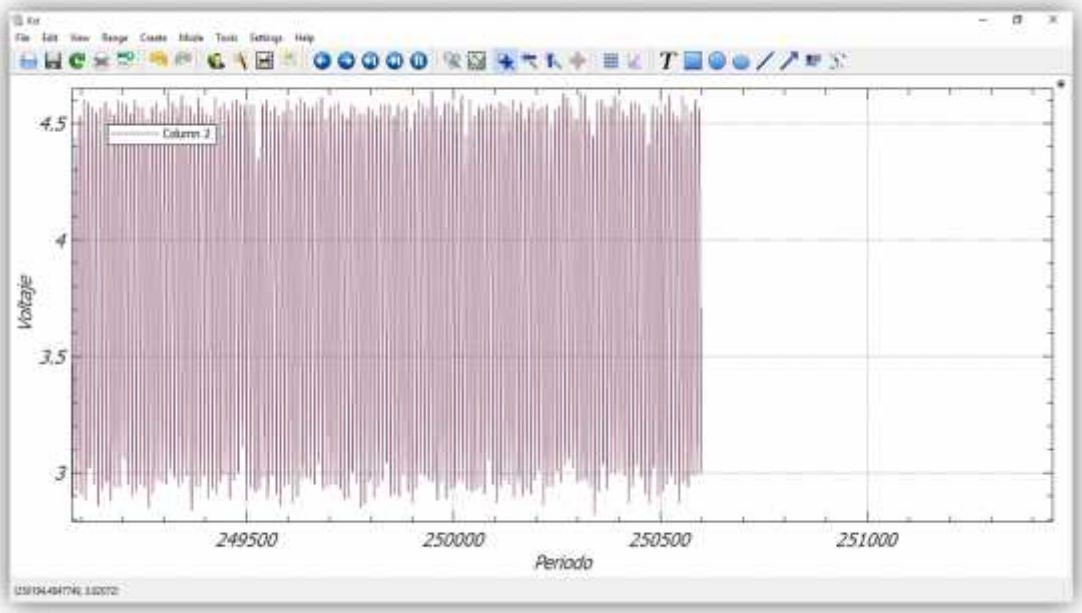


Figura 7-3: ECG 2

Realizado por: Mireya Ramírez **y** Fabricio Jiménez, 2015

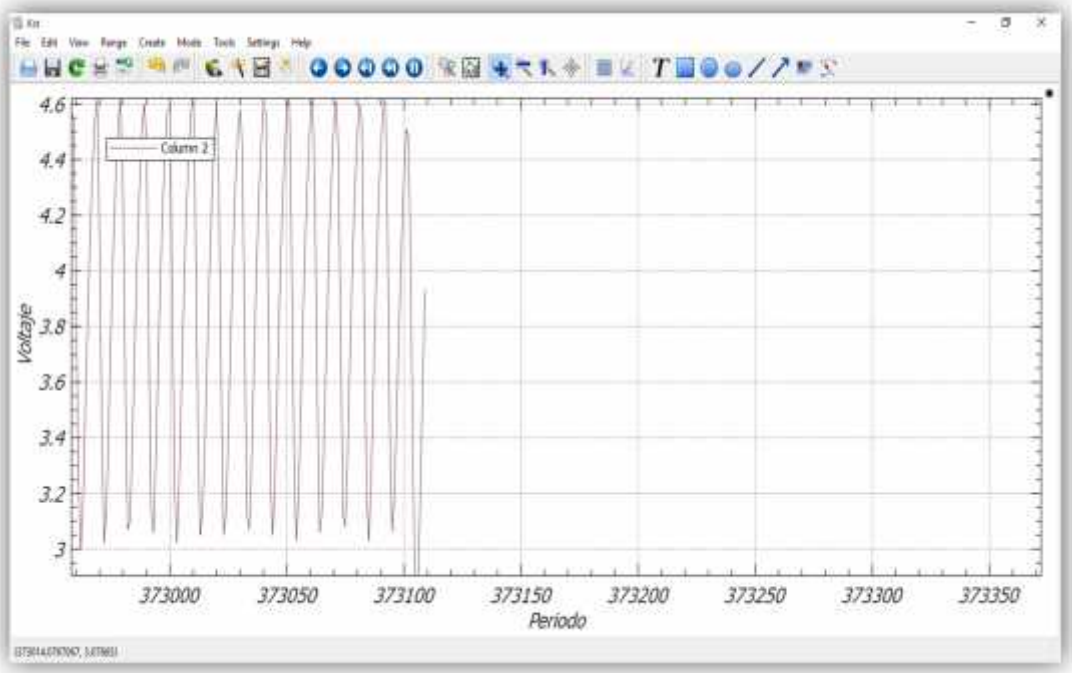


Figura 8-3: ECG 3

Realizado por: M. Ramírez y F. Jiménez, 2015

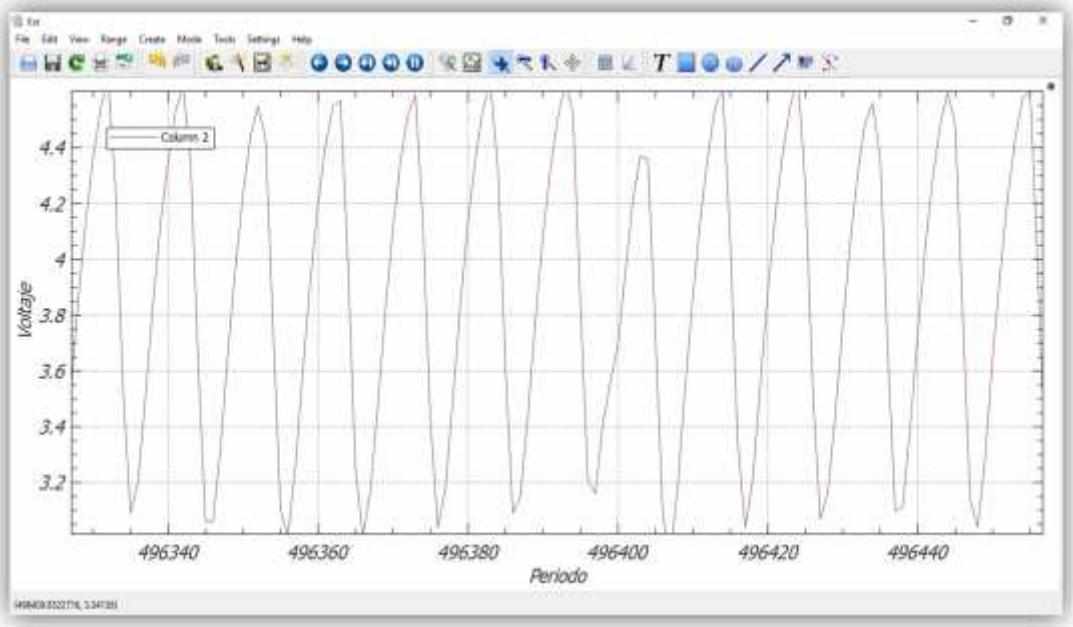


Figura 9-3: ECG 4

Realizado por: M. Ramírez y F. Jiménez, 2015

3.4 Gestión de Seguridad

En el sistema de seguridad se definió las redes y las interfaces tanto interna como externa, efectuando el escenario que se muestra en la Figura 11-3, simulando un ambiente corporativo llamándolo MFSecuEhealth.

Figura 10-3: Logo de Ambiente de Prueba
Fuente: M. Ramírez y F. Jiménez, 2015

Figura 11-3: Ambiente de prueba implementada
Realizado por: M. Ramírez y F. Jiménez, 2015

Para tener una mejor gestión o administración del escenario presentado en la figura 11-3 o red se ha registrado los dispositivos y para reducir los riesgos de responsabilidad se creó perfiles de usuarios con agentes de autenticación y políticas de acceso para un seguimiento.

Figura 12-3: Configuración de Interfaz interna
Realizado por: M. Ramírez y F. Jiménez, 2015

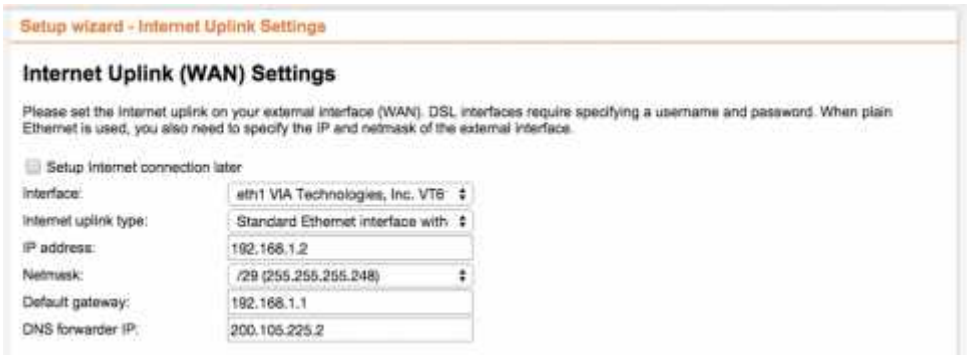


Figura 13-3: Configuración de Interfaz externa
Realizado por: M. Ramírez y F. Jiménez, 2015

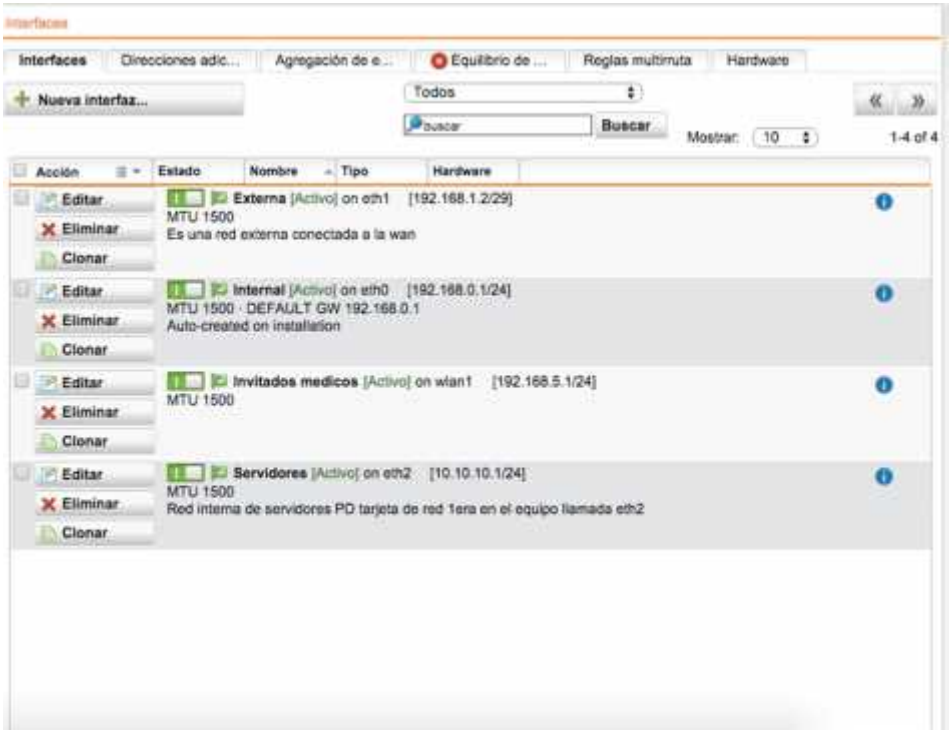


Figura 14-3: Interfaces Configuradas
Realizado por: M. Ramírez y F. Jiménez, 2015

Entre los perfiles de usuarios utilizados se encuentran: Doctores, Personal administrativo, Enfermeras, Administradores de seguridad; mismos que se le asignaron sus privilegios de acceso local y remoto. Al igual que se realizó definiciones de eventos de tiempo para; horarios de trabajo, hora de almuerzo y fines de semana; estas son creadas para ser utilizadas en reglas de filtrado de paquetes y perfiles de seguridad web.

Figura 15-3: Perfiles de Usuario
Realizado por: M. Ramírez y F. Jiménez, 2015

Igualmente se permitió ciertos servicios básicos o predeterminados para los usuarios especificados en la Figura 16-3, además de la creación de un nuevo servicio llamado Transmisión eHealth definiendo el puerto por el que se transmite (8899) y el protocolo de transmisión TCP.

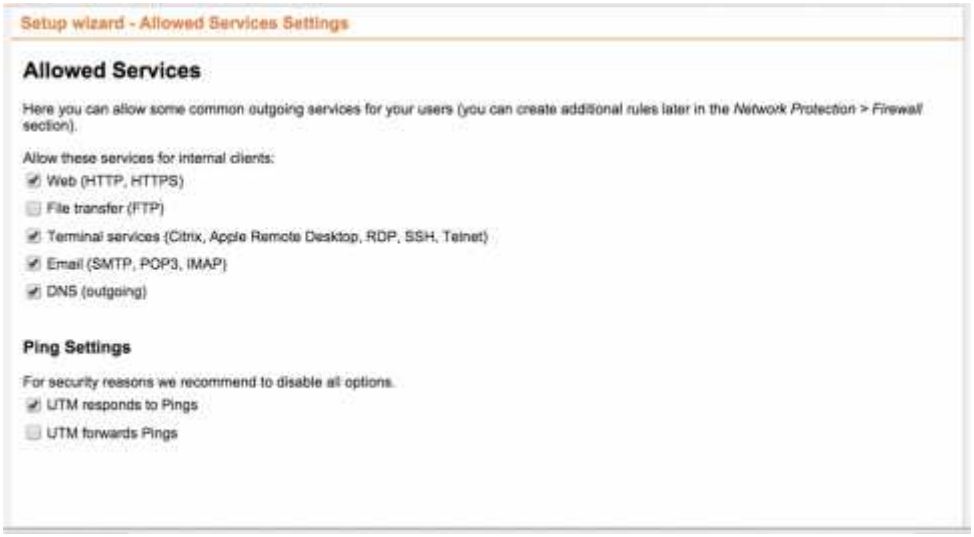


Figura 16-3: Configuración de Servicios
Realizado por: M. Ramírez y F. Jiménez, 2015

Luego de efectuar las definiciones necesarias se procede a configurar la protección de red con funciones de reglas de filtrado y prevenciones de intrusos.

En el firewall se creó una nueva regla de filtrado en el que se definió origen, destino, servicio utilizado y tiempo basado en las políticas de seguridad.

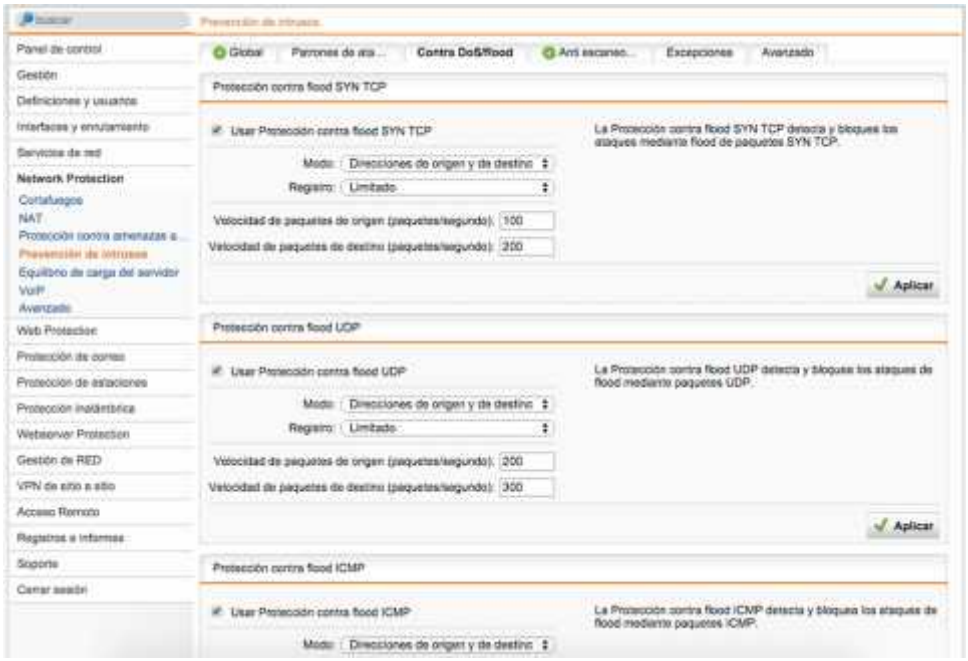


Figura 17-3: Configuración de IPS
Realizado por: M. Ramírez y F. Jiménez, 2015

Se permitió la regla de transmisión desde el dispositivo de telemonitoreo hasta el servidor a través del puerto 8899.

Se activa los registros en tiempo real, de tal manera que verifiquen los paquetes enviados, eliminados y rechazados.

En relación al IPS o Prevención de Intrusos se ha bloqueado el tráfico procedente desde o a otros países basados en la técnica GeoIP Technique que localiza dispositivos en todo el mundo. Además, se activó la protección Snort contra ataques que tratan de explotar debilidades contra servidores, buscadores y ciertas aplicaciones para que genere alertas y realice una acción por defecto.

Figura 18-3: Bloqueo de Tráfico de otros países
Realizado por: M. Ramírez y F. Jiménez, 2015

Para evitar la denegación de servicio y proteger la disponibilidad der sistema se limitó el envío de paquetes por hora en los protocolos TCP, UDP e ICMP utilizando la protección TCP flood, además del anti escaneo de puerto.

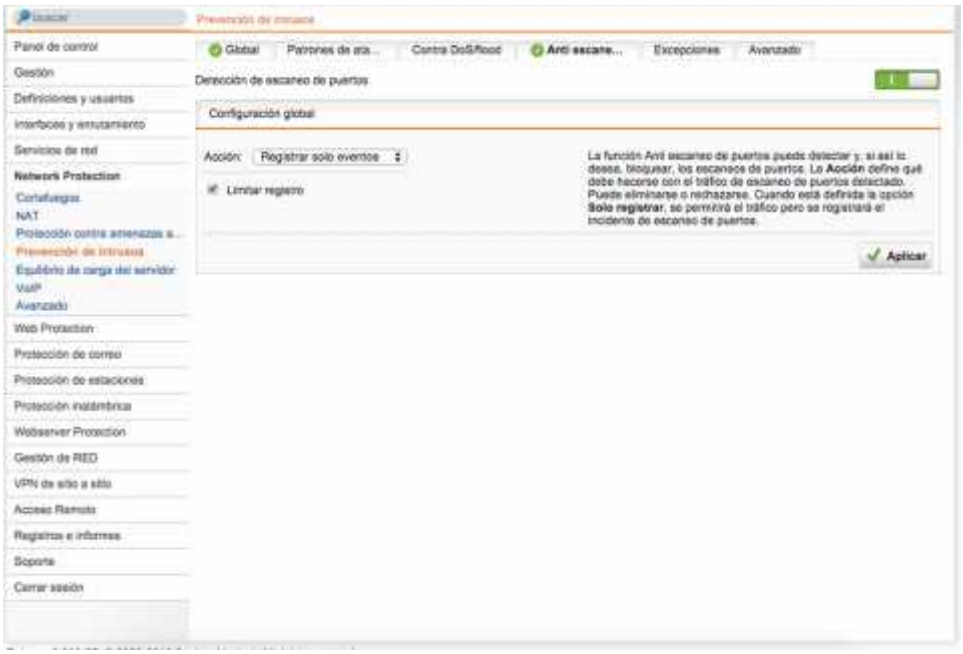


Figura 19-3: Activación de protección de puertos
Realizado por: M. Ramírez y F. Jiménez, 2015

Otra de las configuraciones de IPS son la ICMP que ayuda al control de comunicación entre dos puntos, pero teniendo en cuenta que puede ser malicioso si es aceptado desde redes de poca confianza. En la configuración se controla el comportamiento de paquetes ICMP en la red local.

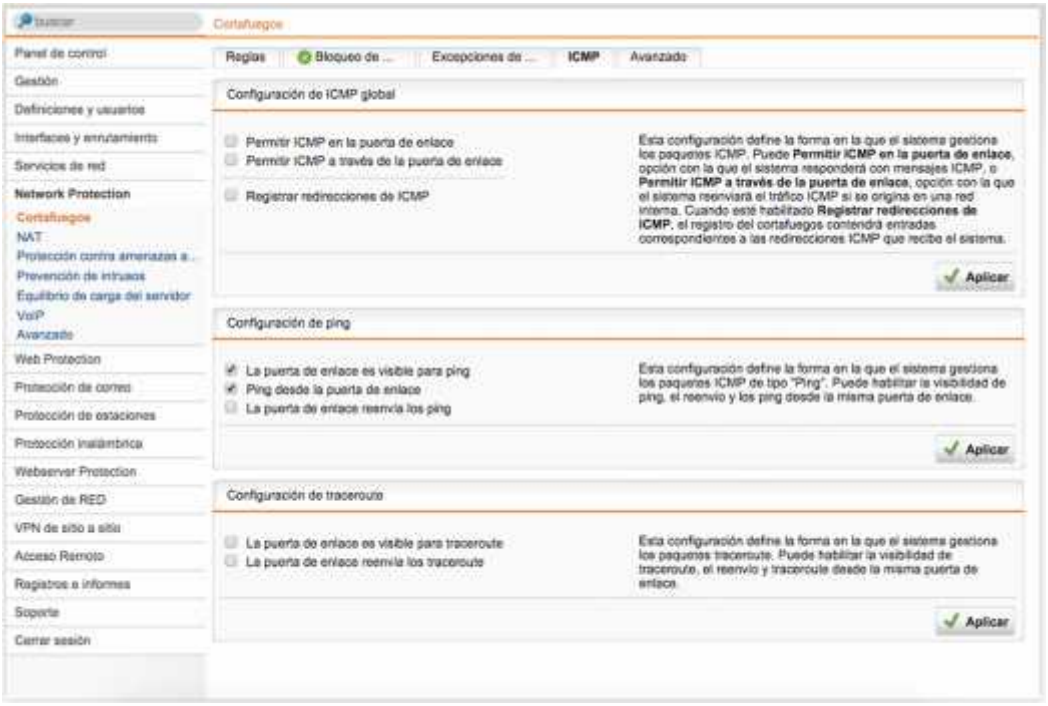


Figura 20-3: Configuración de ICMP
Realizado por: M. Ramírez y F. Jiménez, 2015

Se aplicó configuración de NAT con el fin de ocultar la red interna detrás de una IP pública.

En la Protección Web se controla el acceso a ciertos sitios que llevan contenido nocivo y peligroso como virus, gusanos u otros malware.

Se personalizó la categorización a sitios web de manera que se identifique y bloquee el acceso de los sitios cuestionables. A más de eso se permite la configuración de una lista blanca en la que usuarios, grupos o dominios pueden ser excluidos de ciertos servicios de seguridad y dar permiso a páginas bloqueadas.

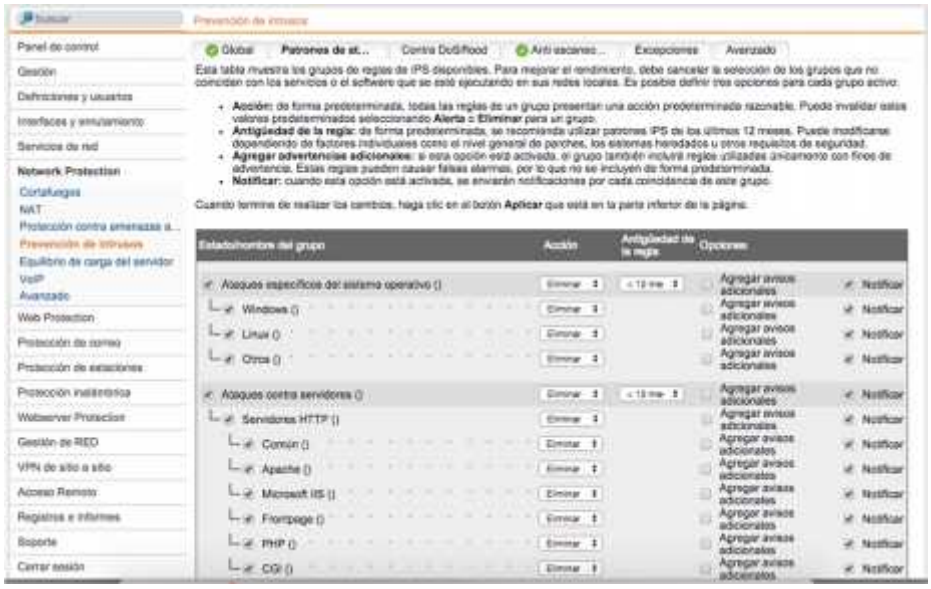


Figura 21-3: Categorización de sitios web
Realizado por: M. Ramírez y F. Jiménez, 2015

Los controles de aplicación son basadas en políticas, permite ver que aplicaciones están siendo utilizadas y por qué usuarios, además de saber quién está ocupando mayores recursos y ralentizando el sistema; de esta manera se puede dar prioridad y clasificar las aplicaciones necesarias para el funcionamiento del sistema.

La protección inalámbrica se realizó para simplificar la operación en las redes, por ello se definió las redes inalámbricas tales como; red de sensores ehealth y red de invitados, estableciendo el método de encriptación empleado. También se especificó el rango de direcciones IP para cada red en un mismo AP. Las direcciones IP asignadas a los clientes sólo se pueden mostrar si Sophos está habilitado como servidor DHCP para la red inalámbrica.

Figura 22-3: Conexiones Inalámbricas
Realizado por: M. Ramírez y F. Jiménez, 2015

Figura 23-3: Clientes Inalámbricos
Fuente: M. Ramírez y F. Jiménez, 2015

Se implementó un servidor real y uno virtual, se aplicó niveles de protección habilitando las medidas que lo protejan contra ataques o comportamiento malicioso. Se permitió el tráfico de datos únicamente de los dispositivos de telemonitoreo registrados.

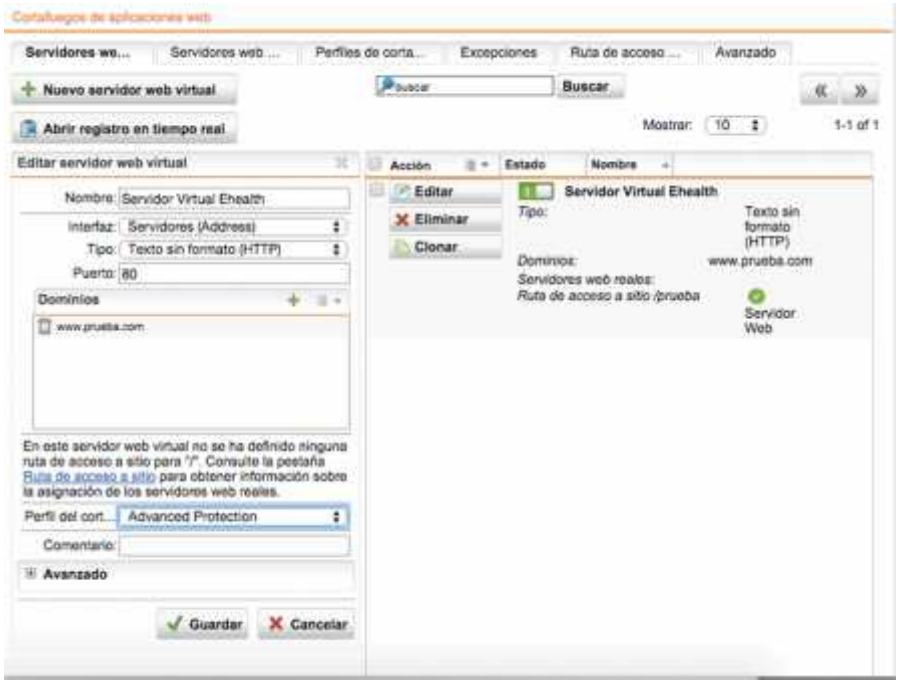


Figura 24-3: Creación de un Servidor
Fuente: M. Ramírez y F. Jiménez, 2015

Para el acceso web se implementó un portal basado en el browser HTML. Los usuarios tendrán acceso remoto seguro a la información en tiempo real sin poder manipularla, a través de la aplicación VNC. Al momento que un usuario accede al portal se le presenta un voucher de invitado en el cual se controla el ingreso por autenticación y se le especifica el tiempo que tiene para la conexión además del tráfico máximo permitido.

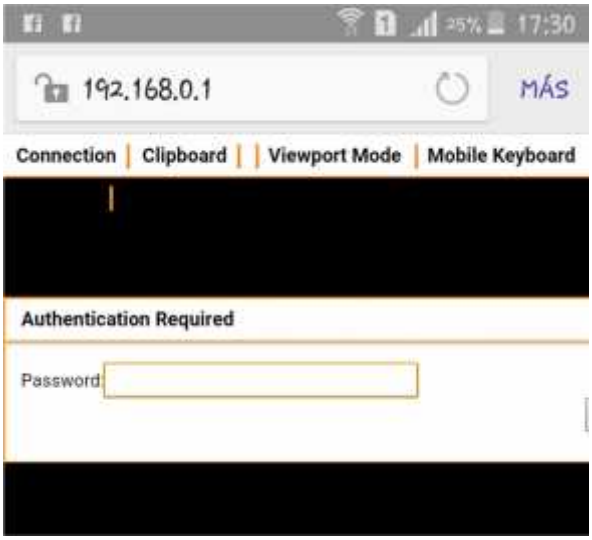


Figura 25-3: Autenticación en acceso remoto
Fuente: M. Ramírez y F. Jiménez, 2015

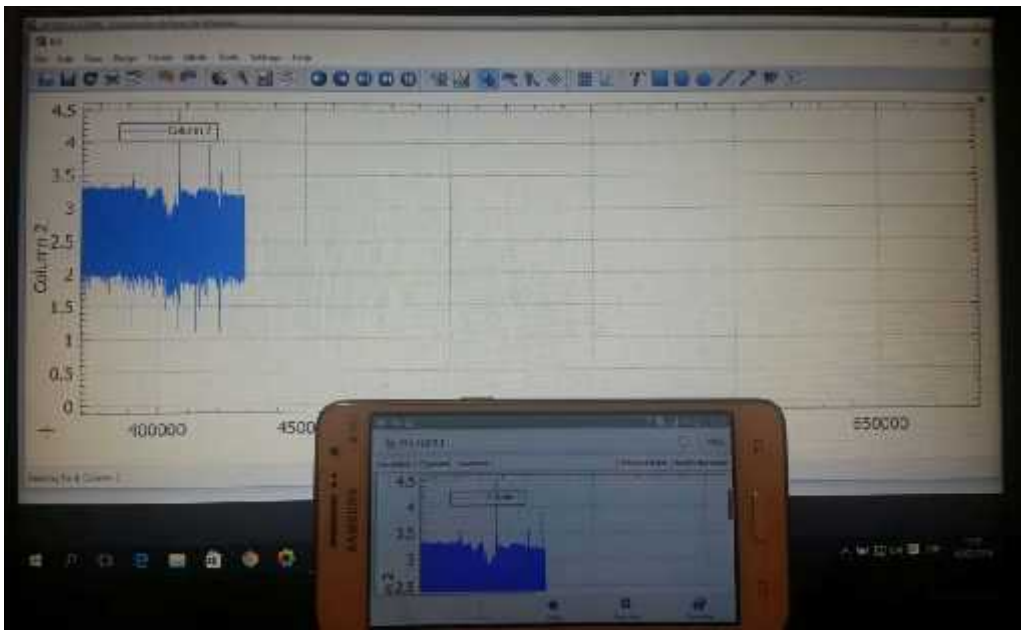


Figura 26-3: Acceso remoto desde Smartphone
Fuente: M. Ramírez y F. Jiménez, 2015

A parte de crear un perfil de prueba se han utilizado herramientas incluidas en el sistema de gestión para comprobar en forma de test las configuraciones y políticas implementadas.

Figura 27-3: Comprobación de ping
Fuente: M. Ramírez y F. Jiménez, 2015

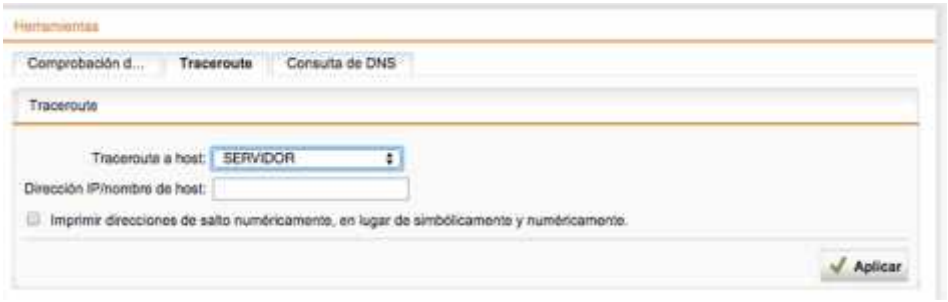


Figura 28-3: Comprobación de Traceroute
Fuente: M. Ramírez y F. Jiménez, 2015

Figura 29-3: Consulta de Ping al Sensor Ehealth
Fuente: M. Ramírez y F. Jiménez, 2015

El sistema proporciona información en tiempo real mediante la recopilación de datos actuales de registro y presentarlo en una forma gráfica, lo que resulta de mucha utilidad al momento de gestionar el sistema. Esta información contiene el análisis histórico y actual de las diversas actividades de la red, y ayuda a identificar las posibles amenazas de seguridad o la solución a problemas.

Otra herramienta utilizada fundamental es la protección de estaciones de trabajo aun cuando no estén conectadas a la red, donde se implementó políticas de control de dispositivos y agentes que amplían la protección registrando y actualizando las definiciones de virus y así bloquear amenazas, programas maliciosos como troyanos trabajando como un IPS en el host. Se

estableció el almacenamiento en dispositivos extraíbles y unidades lógicas con políticas de cifrado a usuarios específicos independientemente de su ubicación.

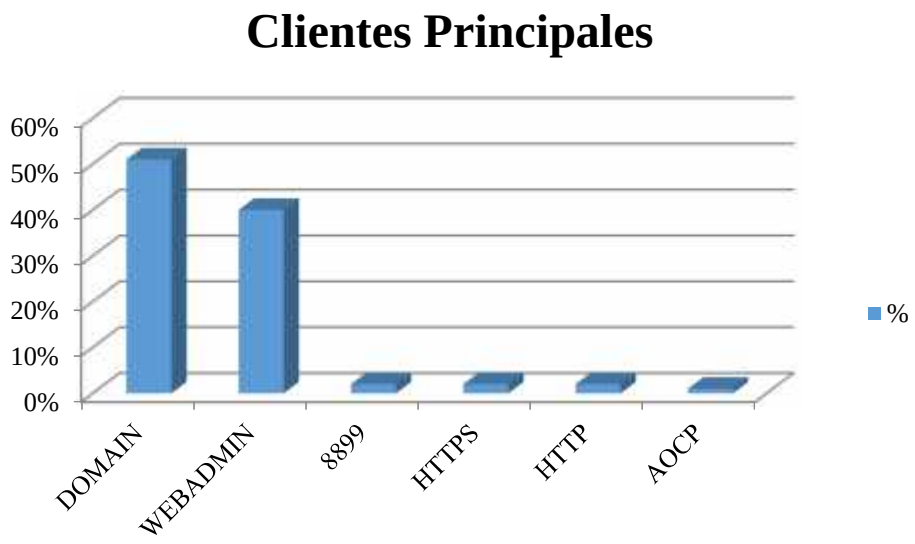
Uso de Red

A continuación, se muestra el tráfico desde originado por los clientes más activos, aplicaciones, servidores y servicios tomados en un tiempo determinado a modo de prueba.

Tabla 11-3: Clientes Principales

Total de paquetes: 40618						
Tráfico total: 3.1 Gb						
		IP	**Usuario/host**	**Paquetes**	**Tráfico**	**%**
1		192.168.0.2	AP EHEALTH	121	15.4 MB	8 %
2		192.168.5.4	192.168.5.4	136	9.0 MB	11 %
3		192.168.0.3	SENSOR EHEALTH	1214	52.8 MB	19 %
4		10.10.10.10	SERVIDOR EHEALTH	35439	2.4 GB	40 %
5		192.168.0.4	Macbook	3706	73.8 MB	21 %
6		192.168.5.1	Invitados medicos (Address)	2	<0.1 MB	1 %

Realizado por: M. Ramírez y F. Jiménez, 2015



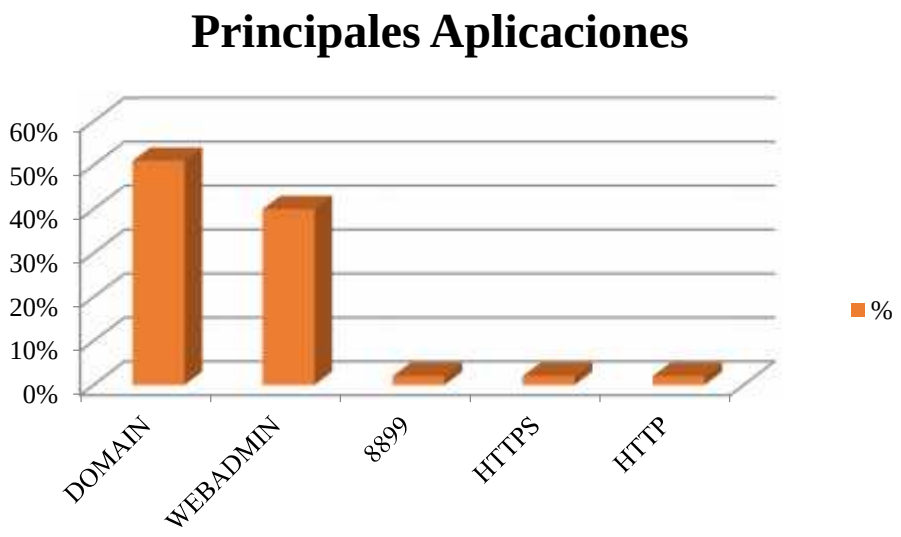
Gráfica 2-3: Clientes Principales

Realizado por: M. Ramírez y F. Jiménez, 2015

Tabla 12-3: Principales Aplicaciones

Total de paquetes: 290				
Tráfico total: 27.5 Mb				
	Aplicación	**Paquetes**	**Tráfico**	**%**
1	Sophos Wireless	108	13.5 MB	49%
2	Unauthorized Hotspot client	138	9.0 MB	33%
3	Unclassified	13	1.9 MB	7%
4	DNS	27	1.7 MB	6%
5	DHCP	4	1.3 MB	5%

Realizado por: M. Ramírez y F. Jiménez, 2015



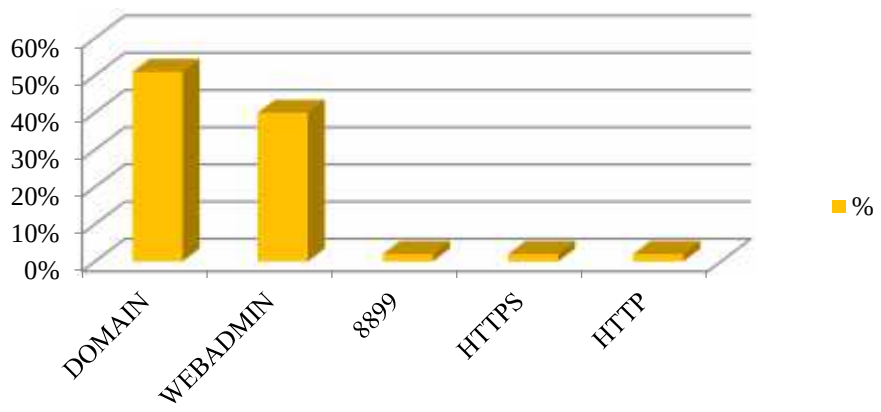
Gráfica 3-3: Principales Aplicaciones

Realizado por: M. Ramírez y F. Jiménez, 2015

Tabla 13-3: Principales Servidores

Total de paquetes: 39561						
Tráfico total: 27.5 Kb						
		IP	**Usuario/host**	**Paquetes**	**Tráfico**	**%**
1		192.168.0.1	Internal (Address)	3980	16.0 MB	26 %
2		192.168.5.1	Invitados medicos (Address)	136	9.0 MB	10 %
3		255.255.255.255	255.255.255.255	4	1.3 MB	5 %
4		10.10.10.1	Servidores (Address)	35439	2.4 GB	58 %
5		192.168.5.4	192.168.5.4	2	<0.1 MB	1 %

Realizado por: M. Ramírez y F. Jiménez, 2015



Gráfica 4-3: Principales Servidores

Realizado por: M. Ramírez y F. Jiménez, 2015

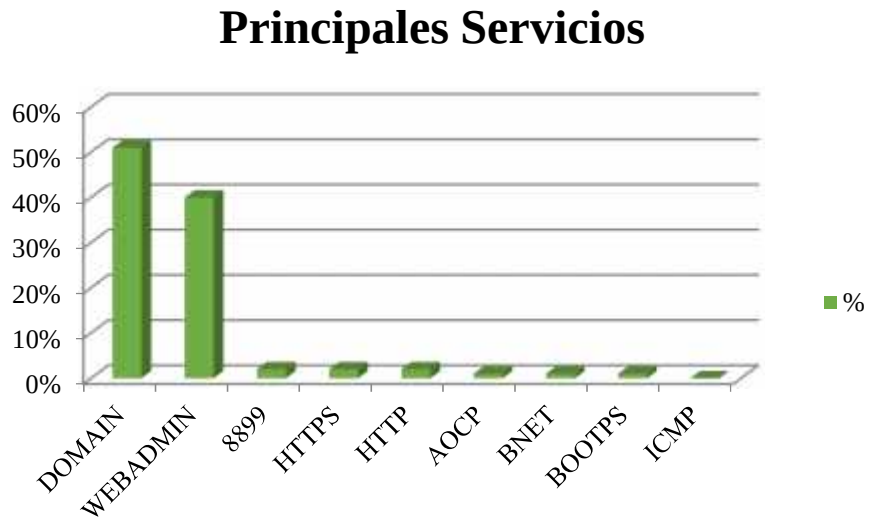
Tabla 14-3: Principales Servicios

Total de paquetes: 40 633

Tráfico total: 4.5 GB

	Nombre del servicio	Protocolo	Puerto del servicio	Paquetes	Tráfico	%
1	DOMAIN	UDP	53	35 118	2.3 GB	51%
2	WEBADMIN	TCP	4444	3 400	1.9 GB	40%
3	8899	TCP	8899	1 206	73.1 MB	2%
4	HTTPS	TCP	443	90	61.9 MB	2%
5	HTTP	TCP	80	537	52.7 MB	2%
6	AOCP	TCP	2712	221	31.0 MB	1%
7	BNET	UDP	415	45	5.4 MB	1%
8	BOOTPS	UDP	67	8	3.2 MB	1%
9	ICMP	ICMP	0	8	0.7 MB	0%

Realizado por: M. Ramírez y F. Jiménez, 2015



Gráfica 5-3: Principales Servicios

Realizado por: M. Ramírez y F. Jiménez, 2015

Para comprobar la eficiencia de las funciones de seguridad implementadas en el sistema MFSecuEhealth se utilizará una distribución de Linux basada en Debian, Kali Linux. Ésta distribución consta de una variedad de herramientas de la cual se efectúan ataques informáticos contra el sistema.

Figura 30-3: Distribución Kali Linux

Realizado por: M. Ramírez y F. Jiménez, 2015

Monitoreo de tráfico y substracción de clave.

Para auditar el sistema MFSecuEhealth en el escenario propuesto se empieza a testear por segmentos. Se inicia comprobando la seguridad en la conexión entre el dispositivo médico y la señal inalámbrica RED EHEALTH que se ha creado en el Punto de Acceso.

En el terminal de comandos se ingresa *iwconfig* con el fin de saber las tarjetas con capacidad WI-Fi que tiene la PC. En la figura 31-3 se puede notar que se cuenta con una tarjeta USB externa que servirá para realizar el **pentesting** del sistema. Se intentará obtener la contraseña de la RED EHEALTH a través de un monitoreo

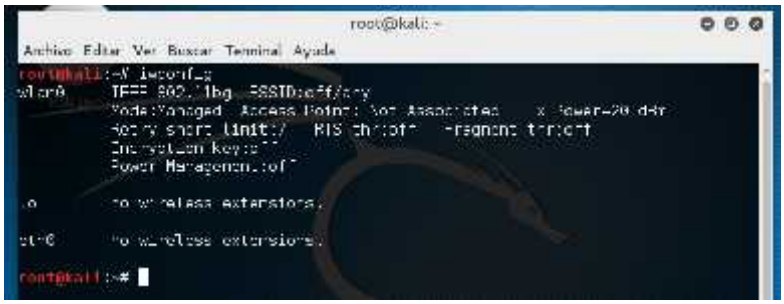


Figura 31-3: Verificando las tarjetas con capacidad Wi-Fi
Realizado por: M. Ramírez y F. Jiménez, 2015

Se coloca la tarjeta de red en modo monitor con el comando *airmon-ng* lo que posteriormente permitirá husmear el tráfico de paquetes. Al cambiar el modo de trabajo de las tarjetas aparecen procesos que pueden causar conflicto con las acciones a realizar, por lo que se los debe matar con el comando *kill* seguido del número del proceso

Figura 32-3: Cambio a modo monitor
Realizado por: M. Ramírez y F. Jiménez, 2015

Una vez cambiado el modo de las tarjetas se procede a husmear el tráfico en todo el entorno con el comando **airodump-ng wlan0mon**

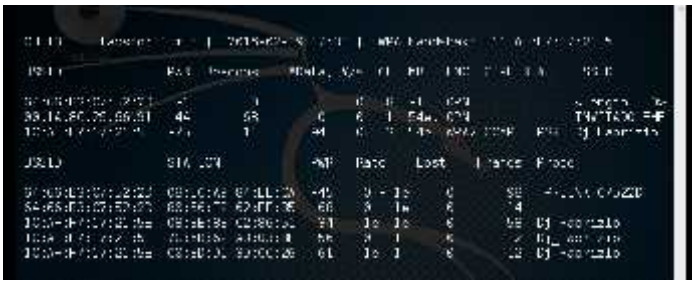


Figura 33-3: Buscando el tráfico de paquetes. RED EHEALTH oculta
Realizado por: M. Ramírez y F. Jiménez, 2015

En el sistema una de las reglas aplicadas fue ocultar la red y solo permitir la conexión de dispositivos registrados con la dirección física (MAC) en una lista blanca. Para comprobar la efectividad de lo dispuesto se analizó el tráfico con la red visible y con la red oculta.

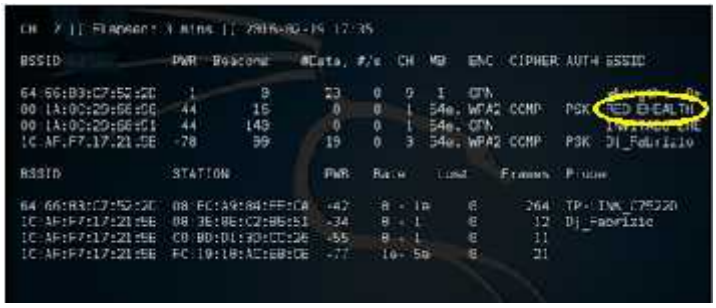


Figura 34-3: Buscando el tráfico de paquetes. RED EHEALTH visible
Realizado por: M. Ramírez y F. Jiménez, 2015

Esta regla de seguridad es muy útil ya que disminuye considerablemente ataques directos en vista de que no es fácil monitorear la red.

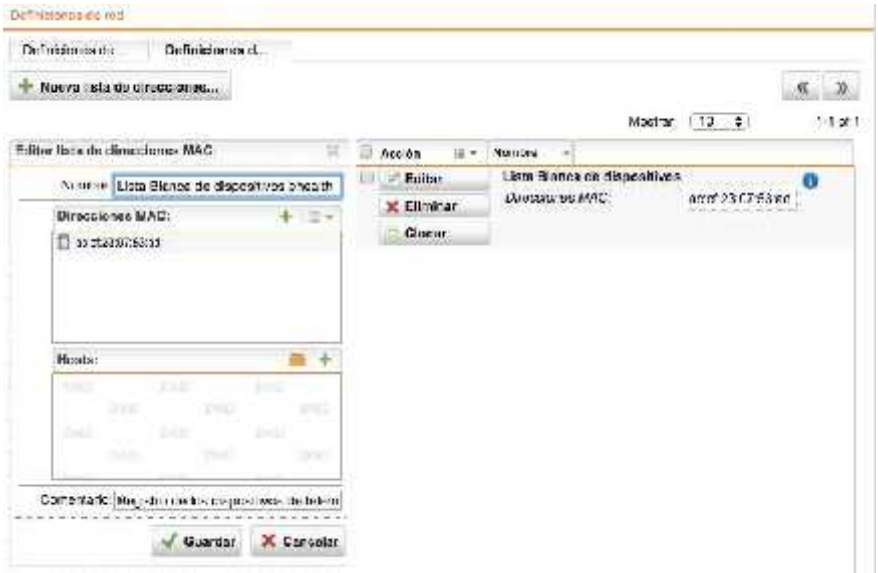


Figura 35-3: Lista Blanca en Definiciones de Red
Realizado por: M. Ramírez y F. Jiménez, 2015

Escaneo de puertos usando NMAP

Se realiza un escaneo de puertos a un host de la red con el fin de auditar la seguridad del sistema y determinar estado de puertos, servicios ofrecidos, existencia de firewall, entre otros. Siendo una de las técnicas más utilizadas para penetrar en un sistema y realizar un previo análisis del mismo, es necesario testear las funciones que controlen este tipo de ataques.
Para ello se utilizó la herramienta NMAP incluida en Kali.

Figura 36-3: Herramienta NMAP en Kali Linux

Realizado por: M. Ramírez y F. Jiménez, 2015

En la línea de comandos se ingresa la instrucción **Nmap –v –A 192.168.0.1** la cual permitirá escanear el estado de los puertos y los servicios.

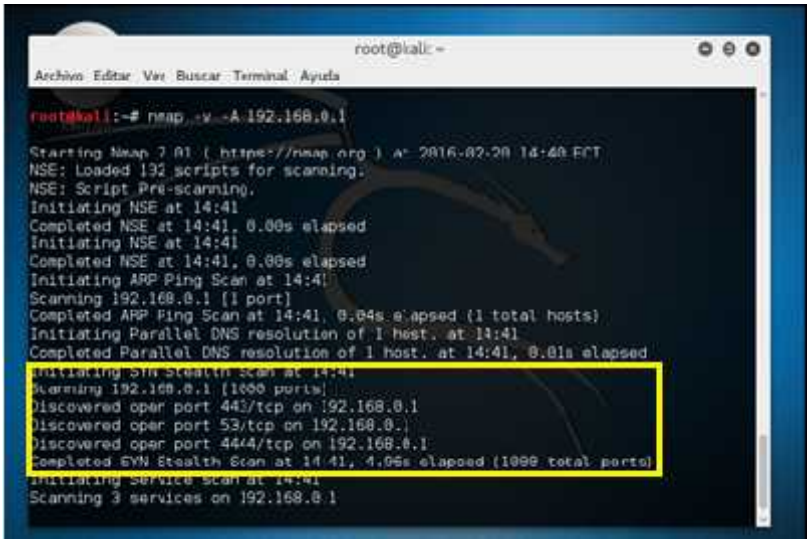


Figura 37-3: Escaneo de puertos

Realizado por: M. Ramírez y F. Jiménez, 2015

Además proporciona información específica del dispositivo. Esto es al desactivar las funciones que restringen este tipo de ataques.

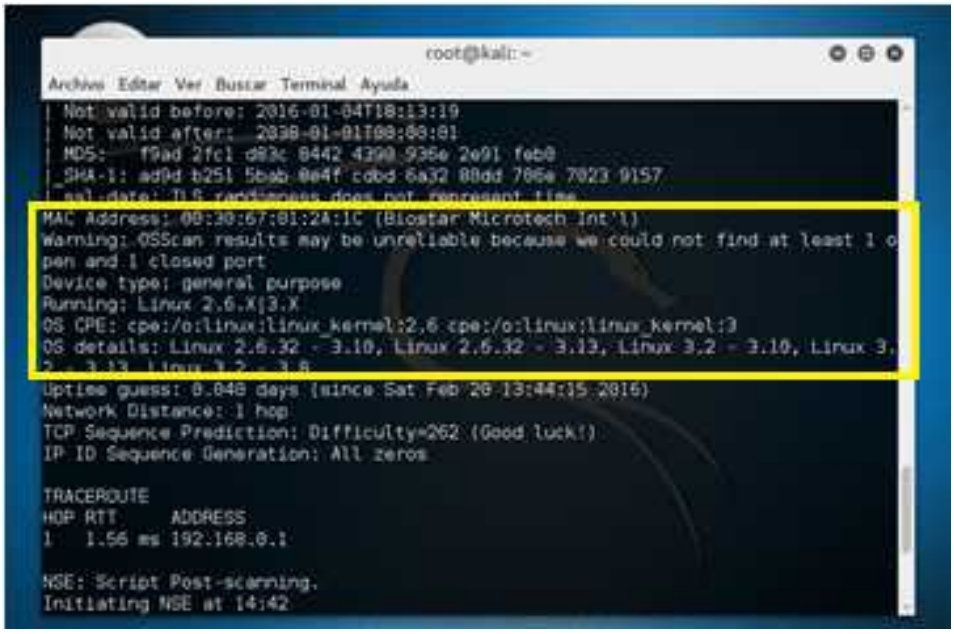


Figura 38-3: Información del host atacado

Realizado por: M. Ramírez y F. Jiménez, 2015

Se activó la función anti escaneo de puertos en el sistema. Al volver a realizar el ataque, esta función realiza un filtrado y se produce un mensaje de error evitando esta acción.

Figura 39-3: Anti escaneo de Puertos

Fuente: M. Ramírez y F. Jiménez, 2015

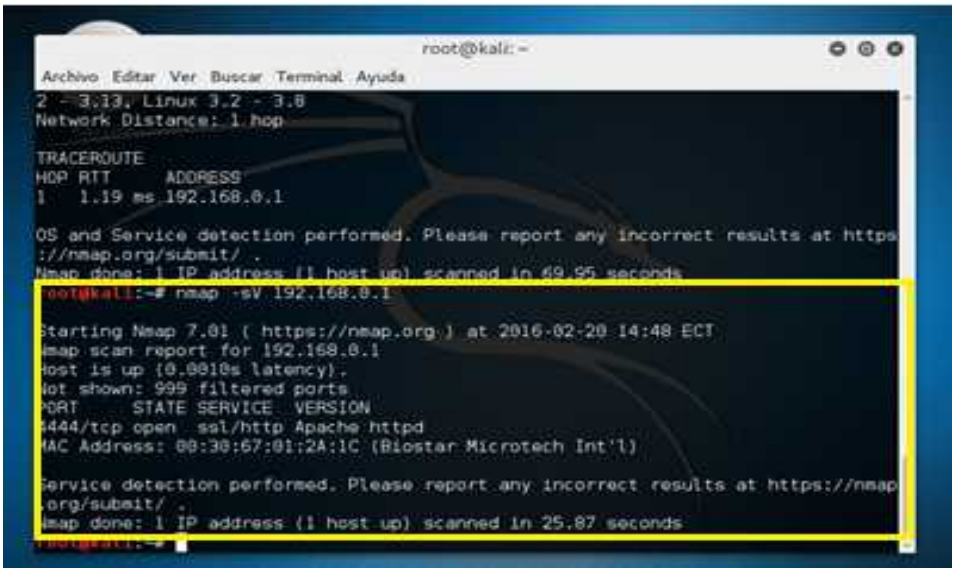


Figura 40-3: Anti escaneo de puertos

Realizado por: M. Ramírez y F. Jiménez, 2015

Inundación de ICMP

Al enviar un alto número de paquetes ICMP se pretende agotar el ancho de banda de la víctima, suponiendo una sobre carga de la red y del sistema de la víctima. Para realizar esta acción se usará la instrucción **hping3** en el modo consola.

La instrucción que se ingresa es la siguiente:

Figura 41-3: Instrucción hping3

Realizado por: M. Ramírez y F. Jiménez, 2015

A través de wireshark se captura los paquetes enviados en pocos segundos a la víctima, causando un aumento en el uso de recursos del sistema agotando del ancho de banda del mismo, tal como se indica en la Figura 42-3.

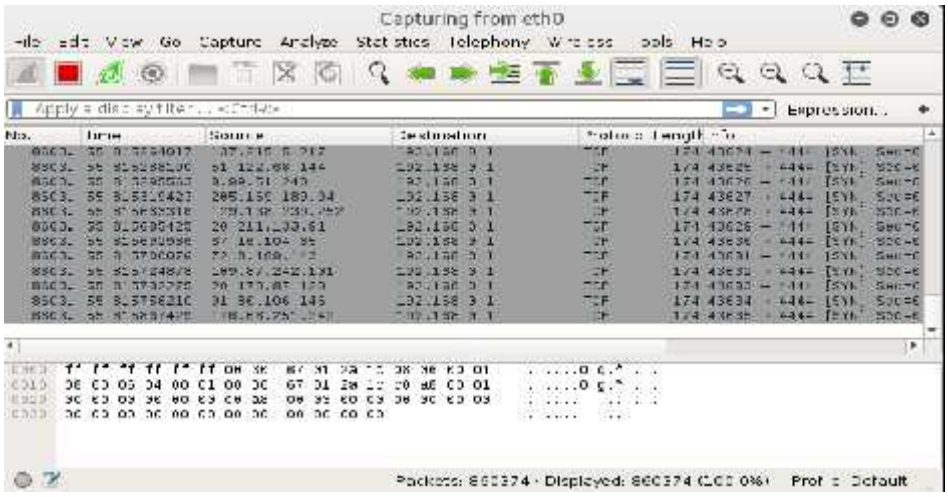


Figura 42-3: Capturas en Wireshark de paquetes enviados
Realizado por: M. Ramírez y F. Jiménez, 2015

Figura 43-3: Uso de Ancho de Banda y Procesamiento
Realizado por: M. Ramírez y F. Jiménez, 2015

Para evitar este tipo de ataques, se implementa una medida de seguridad limitando el número de paquetes ICMP recibidos, de tal manera que rechace y elimine los paquetes restantes.

Figura 44-3: Optimización de Recursos después de aplicar la regla de seguridad
Realizado por: M. Ramírez y F. Jiménez, 2015

Luego de haber realizado un análisis y gestión del riesgo y una determinación del sistema, se realizó una comparación del rendimiento del sistema efectuando ataques informáticos antes y después de implementar las funciones de seguridad.

Tabla 15- 3: Comparación de MFSecuEhealth vs. Sistema no gestionado

Módulos de Seguridad	Funciones	MFSecuEhealth				Sistema no gestionado			
Protección de Redes	Firewall	Alto	8	80%	84%	Bajo	3	30%	36%
	Sistema de Prevención de Intrusos (IPS)	Muy alto	10	100%		Muy Bajo	1	10%	
	Protección avanzada contra amenazas(ATP)	Alto	7	70%		Medio	6	60%	
	VPN de Acceso Remoto Seguro	Alto	8	80%		Bajo	3	30%	
	Portal de Usuarios de autoservicios	Muy Alto	9	90%		Medio	5	50%	
Protección de Redes Inalámbricas	Configuración de múltiples Puntos de Acceso	Muy alto	9	90%	94%	Medio	5	50%	34%
	Red Inalámbrica de alta velocidad fiable	Alto	8	80%		Alto	8	80%	
	Puntos de acceso Wi-Fi para invitados	Muy alto	10	100%		Muy Bajo	2	20%	
	Configuración de lista blanca	Muy alto	10	100%		Muy Bajo	1	10%	
	Máxima protección para el tráfico inalámbrico (Cifrado seguro)	Muy alto	10	100%		Muy Bajo	1	10%	
Protección Web	Políticas de Filtrado URL	Muy alto	9	90%	76%	Bajo	4	40%	28%
	Protección de Malware en internet	Medio	5	50%		Bajo	3	30%	
	Activación de reglas para protección integra de la red	Muy alto	10	100%		Muy Bajo	1	10%	
	Políticas de autenticación por tipo de dispositivo	Alto	7	70%		Bajo	3	30%	
	Clasificación de sitios web: confianza, neutro, malintencionado y sospechoso	Alto	7	70%		Bajo	3	30%	
Protección de Estaciones de Trabajo	Antivirus y protección contra programas maliciosos	Medio	6	60%	77%	Medio	5	50%	23%
	Escanea archivos, páginas web, y dispositivos para bloquear amenazas y enviar alertas	Alto	8	80%		Muy Bajo	1	10%	
	Control de dispositivos extraíbles	Muy alto	9	90%		Muy Bajo	1	10%	
Protección de Servidores	Refuerzo de servidores	Muy Alto	10	100%	100%	Muy Bajo	1	10%	10%
	Protección de Información sensible	Muy alto	10	100%		Muy Bajo	1	10%	

Fuente: M. Ramírez y F. Jiménez, 2015

La escala aplicada en la Tabla 15-3 fue la siguiente:

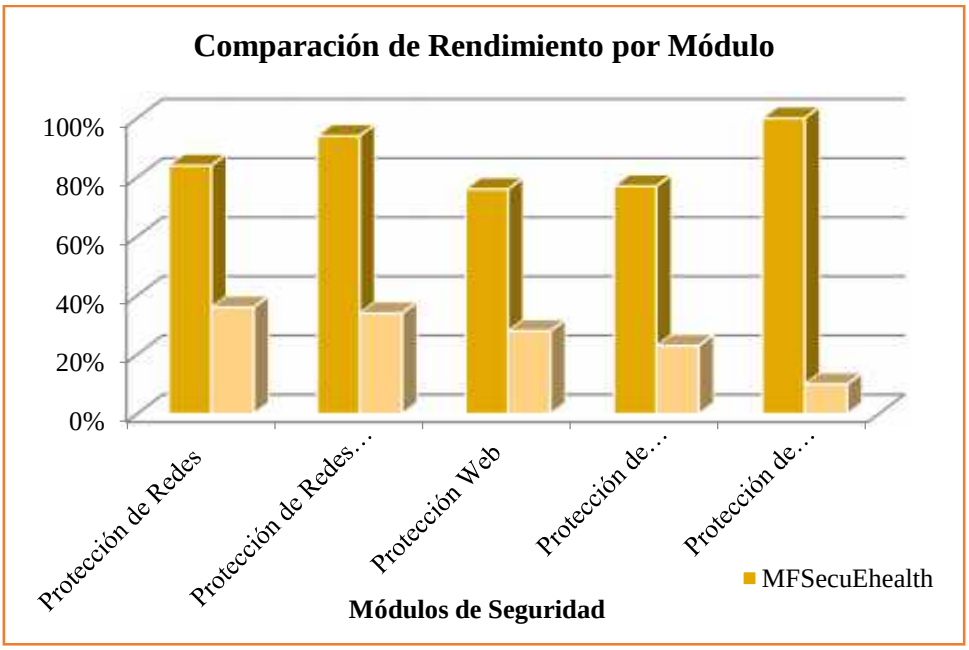
Rendimiento	Escala	%
Muy Alto	9 a 10	90% a 100%
Alto	7 a 8	70% a 80%
Medio	5 a 6	50% a 60%
Bajo	3 a 4	30% a 40%
Muy Bajo	1 a 2	10% a 20%

La siguiente tabla representa un porcentaje promedio del rendimiento por módulo de seguridad aplicado en el escenario, en el cual se diferencia las mejoras del sistema MFSecueEhealth con respecto a un sistema no gestionado con seguridad.

Tabla 16-3: Comparación de Rendimiento de cada módulo

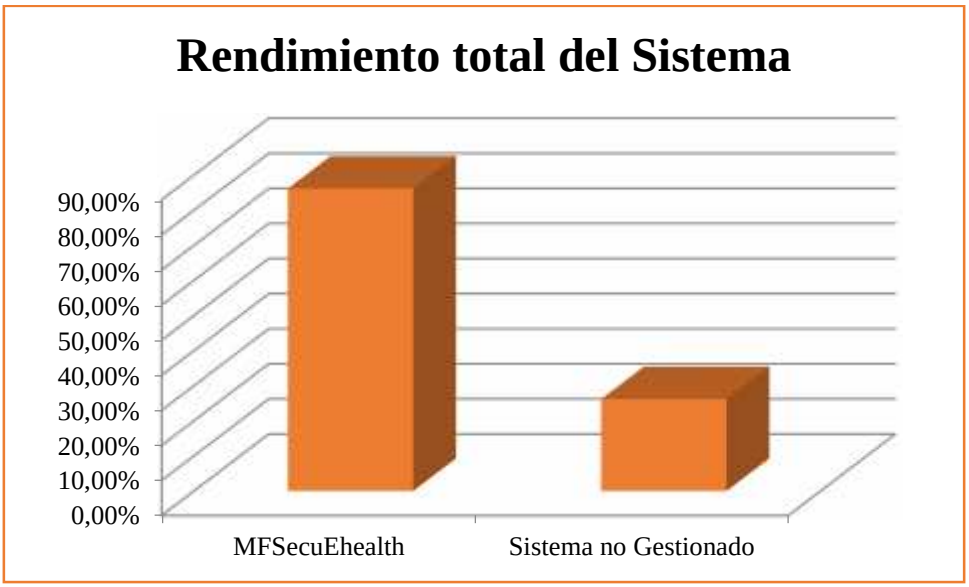
Módulos de Seguridad	MFSecuEhealth	Sistema no Gestionado
Protección de Redes	84%	36%
Protección de Redes Inalámbricas	94%	34%
Protección Web	76%	28%
Protección de Estaciones de Trabajo	77%	23%
Protección de Servidores	100%	10%
Rendimiento total	**86,20%**	**26,20%**

Realizado por: M. Ramírez y F. Jiménez, 2015



Gráfica 6-3: Comparación de Rendimiento por módulo

Realizado por: M. Ramírez y F. Jiménez, 2015



Gráfica 7-3: Rendimiento total del Sistema
Realizado por: M. Ramírez y F. Jiménez, 2015

Una vez realizado la comprobación de la seguridad se obtuvo un sistema eficiente y preparado para actuar contra cualquier tipo de amenazas representando un rendimiento de 86,2% en un Sistema gestionado con seguridad contra un 26,20% de un sistema no gestionado.

CONCLUSIONES

- Se concluye que en un sistema de seguridad de telemonitoreo se deben considerar aspectos técnicos ya que el riesgo en una organización nunca es eliminado solo mitigado, por lo cual es importante mantenerse actualizado en cuanto a las nuevas amenazas que atenten contra la seguridad de los activos de la empresa.

- Para diseñar un buen sistema de gestión de seguridad se debe recurrir a la norma ISO 27001, éste define las pautas para ejecutar una estructura de seguridad completa enmarcando, hardware, software y servicios.

- El ambiente de prueba propuesto para este trabajo de tesis está diseñado de tal manera que simule un ambiente real. Este sistema brinda eficiencia en la toma de datos por telemonitoreo teniendo un tiempo de retardo casi imperceptible y un consumo de recursos técnicos mínimo.

- Al implementar la gestión de seguridad es importante realizar un análisis de los riesgos y requerimientos del sistema. En el ambiente de prueba el cumplimiento de los requerimientos fue de 71%, lo que posteriormente nos permitió la obtención de un rendimiento de 86.20% de recursos y efectividad en la seguridad.

- La implementación de políticas de seguridad es siempre una excelente medida para disminuir y prevenir el riesgo en las empresas. Estas medidas deben ser acatadas por todos los miembros de una organización.

RECOMENDACIONES

Luego de implementar y analizar lo expuesto en este trabajo se recomienda lo siguiente:

- Antes de implementar un prototipo de telemonitoreo es importante averiguar si se cuenta con la tecnología necesaria para dicho fin. Es importante recalcar que cada dispositivo cuenta con sus librerías y guías de uso para su aplicación, mismas que no servirán si no se las emplea de manera correcta.

- Se recomienda que antes de implementar un sistema de seguridad se realice una valoración de los activos y de la inversión a realizar de tal modo que exista un equilibrio, es decir, que el gasto en seguridad no sea mayor que el valor de los activos a proteger.

- Antes de implementar una regla de seguridad se recomienda crear perfil es de prueba que no afecten el funcionamiento del sistema general, una vez evaluada la nueva regla aplicar.

- Aplicar la guía de políticas de seguridad propuesta para salvaguardar la información, y actualizarla o modificarla cada cierto tiempo.

BIBLIOGRAFÍA

1. ALVARADO LEÓN, Sergio Israel, & JUÁREZ CUEVAS, David Ángel. *Redes de Área Corporal en el Cuidado de la Salud* [en línea] (Tesis) (Ingeniería). Universidad Nacional Autónoma de México, Facultad de Ingeniería. México, DF, 2012, pp. 25-47, 64. [Consulta: 25-02-2015]. Disponible en: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2568/Tesis.pdf?sequence=1

2. CARACTERISTICAS TÉCNICAS DE ARDUINO UNO. [blog]. [Consulta: 13-03-2015]. Disponible en: http://www3.gobiernodecanarias.org/medusa/ecoblog/ralvgon/files/2013/05/Caracter%C3%ADsticas-Arduino.pdf

3. CISCO CERTIFIED. *Seguridad de las Redes* [digital]. Versión 1.1. pp. 189-198, 239-243, 249-252

4. CISCO NETWORKING ACADEMY. *Seguridad de la Red* [digital]. pp. 36-40

5. ENCICLOPEDIASALUD. *Electrocardiograma* [en línea]. [consulta: 17-03-2015]. Disponible en: http://www.enciclopediasalud.com/definiciones/electrocardiograma

6. FERNÁNDEZ, Ándres. "TIC y Salud: Promesas y Desafíos para la inclusión social". *Newsletter* [en línea], 2010, (Unión Europea), volumen (12), pp. 2-3. [Consulta: 3-03-2015]. Disponible en: http://www.cepal.org/socinfo/noticias/paginas/3/44733/newsletter12.pdf

7. GUTIERREZ, Alejandro; et al. *Sistema Prototipo de Telemonitoreo para pacientes, Usando Tecnologías Inalámbricas Semimóviles de Comunicación* [en línea] (tesis) (ingeniería). Pontificia Universidad Javeriana, Facultad de Ingeniería. Colombia, Bogota, 2005, pp 41-42. [Consulta: 10-03-2015]. Disponible en: http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis105.pdf

8. JAMIL Y, Khan; & MEHMET R, Yuce. *New Developments in Biomedical Engineering* [en línea]. Australia: Domenico Campolo, 2010. [Consulta: 20-02-2015]. Disponible en:

http://www.intechopen.com/books/new-developments-in-biomedical-engineering/wireless-body-area-network-wban-for-medical-applications

9. JIMENÉZ HERRANZ, Jesús. *Conceptos en seguridad de los sistemas de información: confidencialidad, integridad, disponibilidad y trazabilidad* [en línea]. España: Creative Commons Atribución-LicenciarIgual. [Consulta: 2-04-2015]. Disponible en: http://oposcaib.wikispaces.com/file/view/38++Conceptes+en+seguretat+dels+sistemes+d'informaci%C3%B3.+Confidencialitat,+integritat,+disponibilitat+i+tra%C3%A7abilitat.pdf

10. LAS REDES INALÁMBRICAS [en línea]. [Consulta: 11-03-2015]. Disponible en: http://www.informaticamoderna.com/Redes_inalam.htm

11. MARTINEZ RAMOS, Carlos. "Telemedicina. Aspectos Generales". *Reduca (Recursos Educativos)* [en línea] 2009, (Madrid), pp. 61-65. [Consulta: 2-03-2015]. Disponible en: http://www.revistareduca.es/index.php/reduca/article/viewFile/7/4

12. MENESES, Andrés, & PARRA, Sergio. *Análisis de Riesgo Seguridad Informática* [en línea]. 2015. [Consulta: 5-04-2015]. Disponible en: http://inacap.serveftp.com/tic/Exposiciones_N1/AGR.pdf

13. PARRAGA NUÑEZ, Víctor Allan. *Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de ingeniería de sistemas computacionales, basado en el análisis de su infraestructura de red interna y de perímetro* (tesis) (ingeniería)[en línea]. Universidad de Guayaquil, Ecuador 2014.pp. 54-56. [Consulta: 25-04-2015]. Disponible en: http://repositorio.ug.edu.ec/bitstream/redug/6672/1/TesisCompleta-536-2014.pdf

14. PLACA ARDUINO UNO. [en línea]. 2012 [Consulta: 13-03-2015]. Disponible en: http://www.menosmedia.org/spip.php?article43

15. RABANALES, Joseaba; et al. "Tecnologías de la Información y las Comunicaciones: Telemedicina". *Revclinmedfam* [en línea] 2010, (España), p 42. [Consulta: 2-03-2015]. Disponible en: http://www.revclinmedfam.com/PDFs/cfecdb276f634854f3ef915e2e980c31.pdf

16. RASPBERRY PI. *E-Health Plataforma V2.0 para Arduino y Raspberry Pi para aplicaciones médicas* [en línea]. Admin: 2013. [Consulta: 13-03-2015]. Disponible en: http://www.raspberryshop.es/wp/e-health-plataforma-v2-0-para-arduino-y-raspberry-pi-para-aplicaciones-medicas/

17. RFcom. Ca. *Tasa de Absorción Especifica de los teléfonos inalámbricos* [en línea]. [Consulta: 22-02-2015]. Disponible en: http://www.rfcom.ca/primer/sarsp.shtml

18. SATURACION DE OXÍGENO. [en línea]. [Consulta: 17-03-2015]. Disponible en: http://www.mimoonline.es/pregunta.php?idP=48

19. SENSORES MÉDICOS. [en línea]. [Consulta: 13-03-2015]. Disponible en: http://www.medipense.com/es/medisense/

20. SHANGHAI WAFER MICROELECTRONICS CO., LTD. [en línea]. [Consulta: 11-03-2015] Disponible en: http://www.waferstar.com/downloads/WIFI232-A11-V4.0-EN.pdf

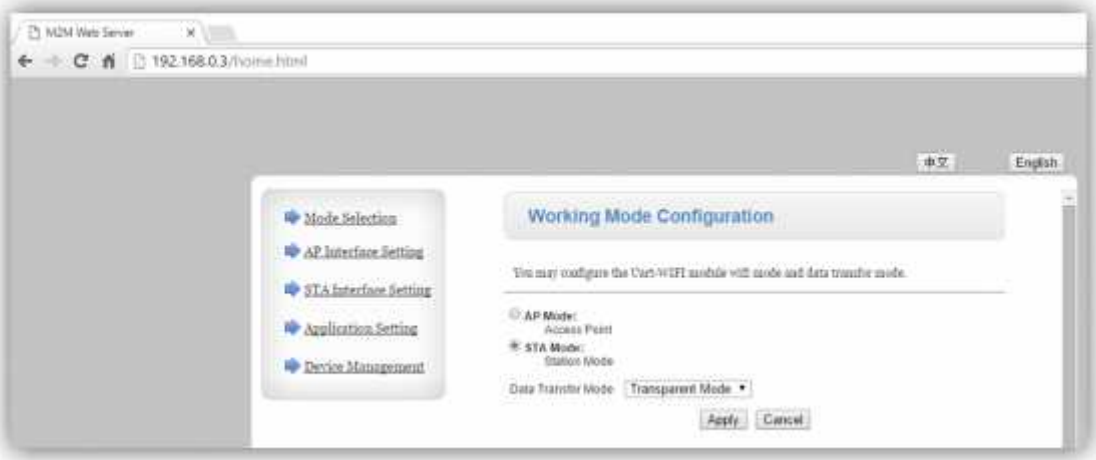
21. TECNOLOGÍA WIFI [en línea]. [Consulta: 11-03-2015]. Disponible en: http://www.ecured.cu/Tecnolog%C3%ADa_Wi-Fi

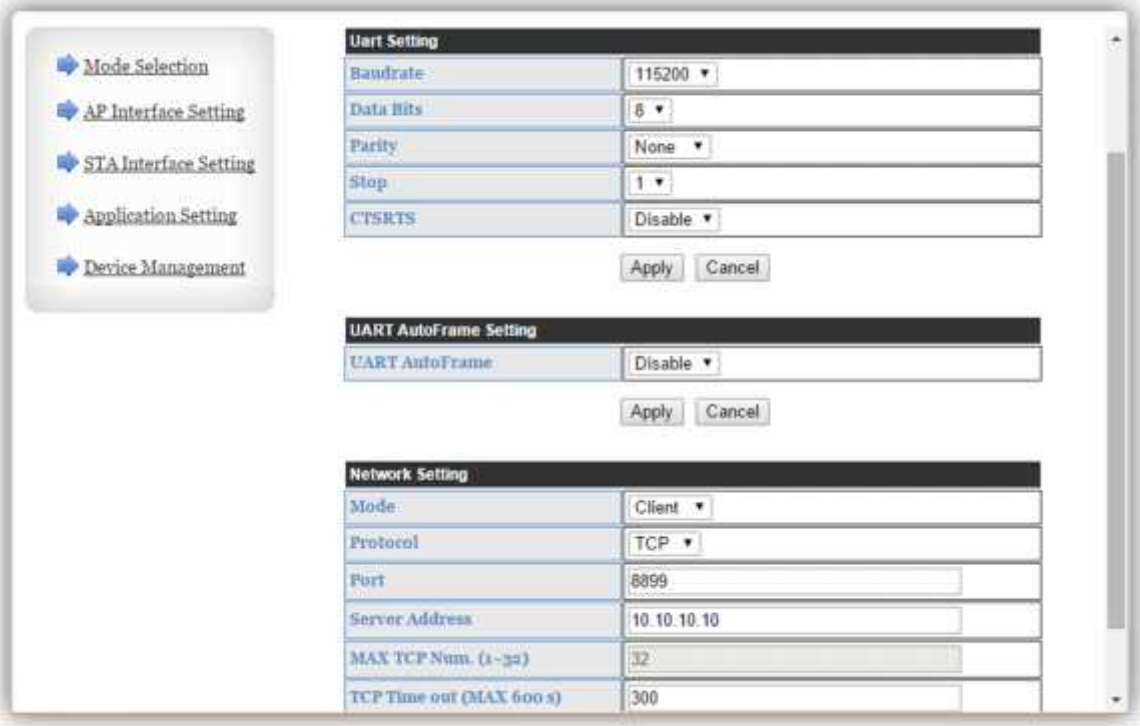
22. TECNOLOGÍA WIFI [en línea]. [Consulta: 11-03-2015]. Disponible en: http://www.tecnowifi.com/

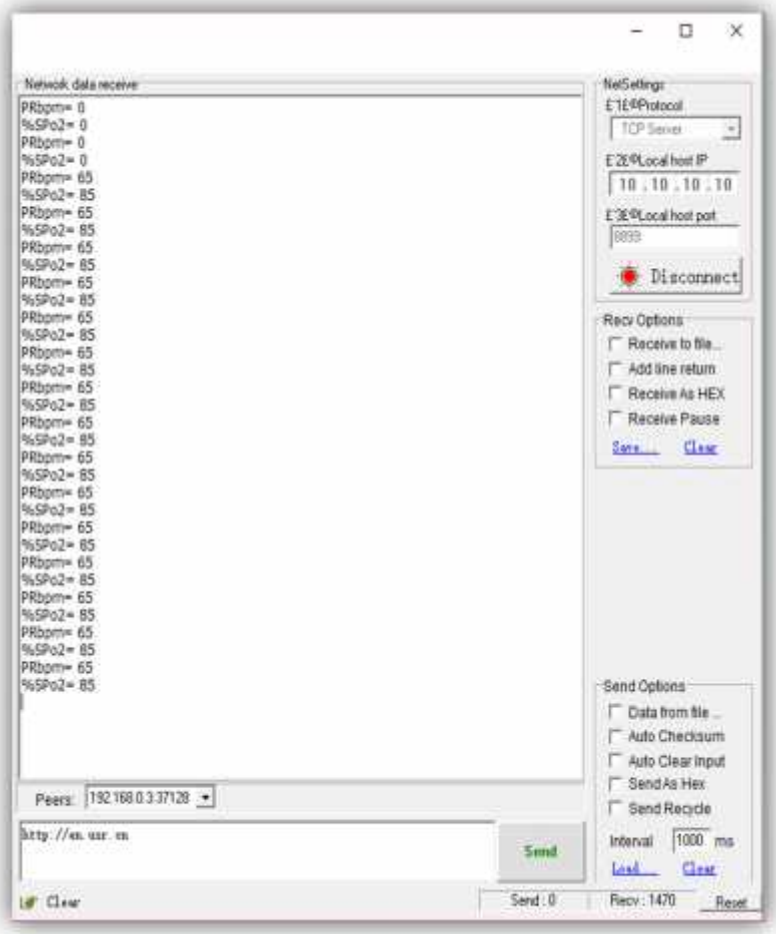
23. WIRELESS & CABLE (WiCa). *Wireless Body Area Network (WBAN)* [en línea]. [Consulta: 20-02-2015]. Disponible en: http://www.wica.intec.ugent.be/research/wireless-body-area-networks

ANEXOS

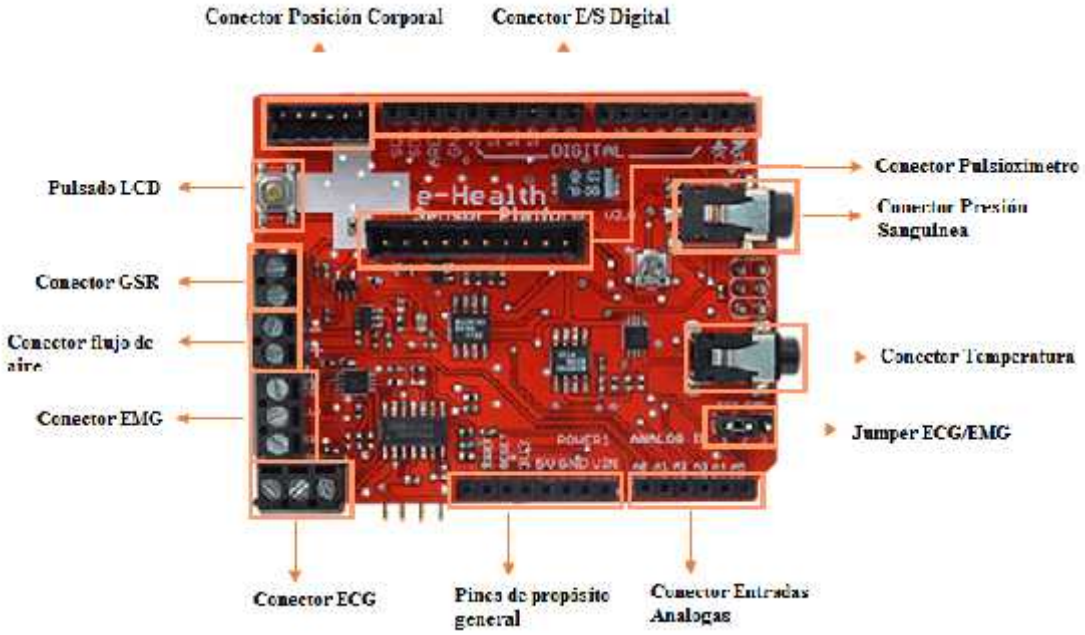
Anexo A. Configuración del módulo Wifi 232-B en modo web



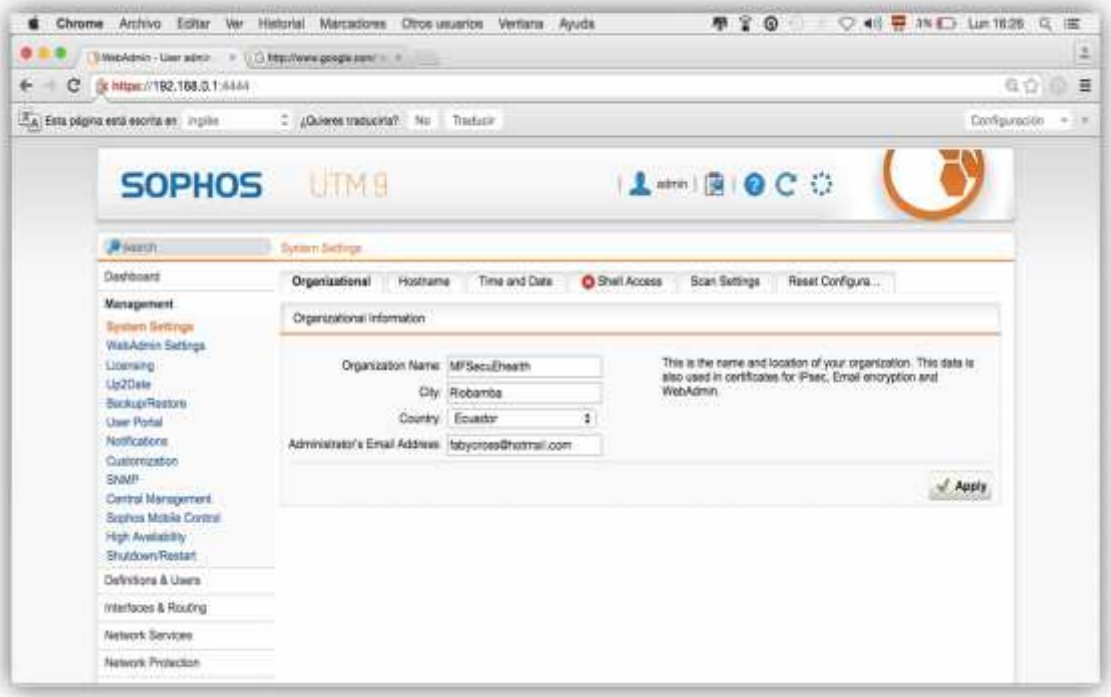

Mode Selection
AP Interface Setting
STA Interface Setting
Application Setting
Device Management
Uart Setting
Baudrate
115200
Data Bits
8
Parity
None
Stop
1
CTSRTS
Disable
Apply
Cancel
UART AutoFrame Setting
UART AutoFrame
Disable
Apply
Cancel
Network Setting
Mode
Client
Protocol
TCP
Port
8899
Server Address
10.10.10.10
MAX TCP Num. (1~32)
32
TCP Time out (MAX 600 s)
300

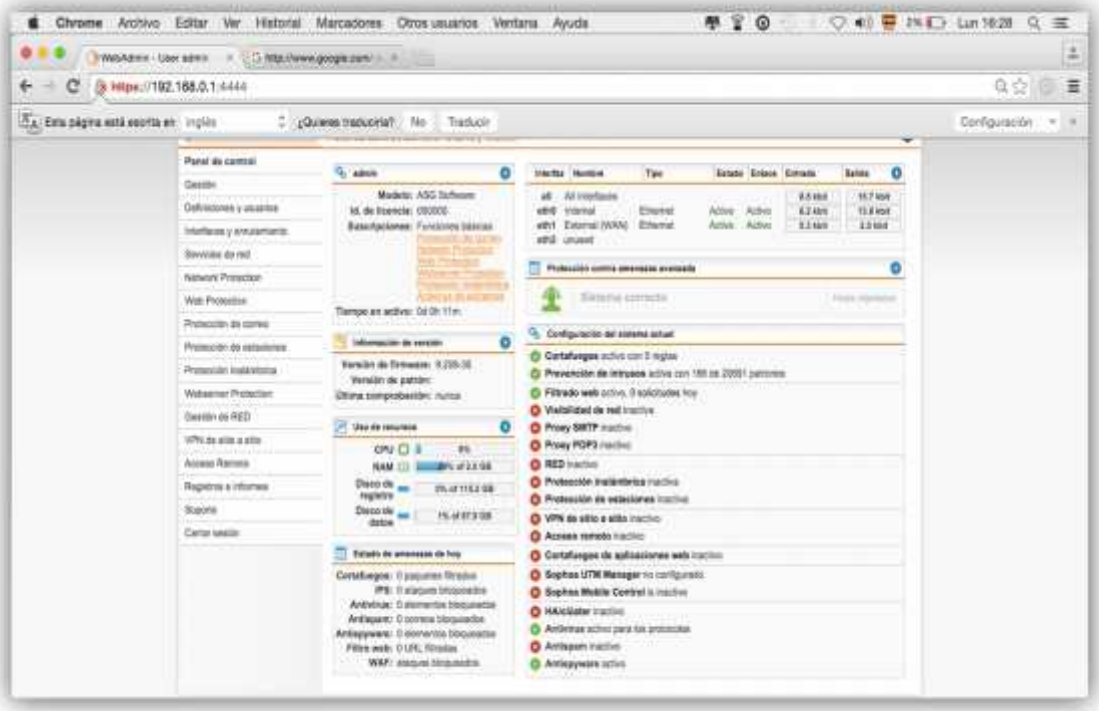

Network data receive
PRbpm= 0
%SPo2= 0
PRbpm= 0
%SPo2= 0
PRbpm= 65
%SPo2= 85
NetSettings
TCP Server
10 . 10 . 10 . 10
8899
Disconnect
Recv Options
Receive to file...
Add line return
Receive As HEX
Receive Pause
Save...
Clear
Send Options
Data from file ...
Auto Checksum
Auto Clear Input
Send As Hex
Send Recycle
Interval
1000
ms
Load...
Clear
Peers:
192.168.0.3:37128
Send
Clear
Send : 0
Recv : 1470
Reset

Anexo B. Plataforma de sensores eHealth



Anexo C. Configuración inicial de Sophos UTM 9

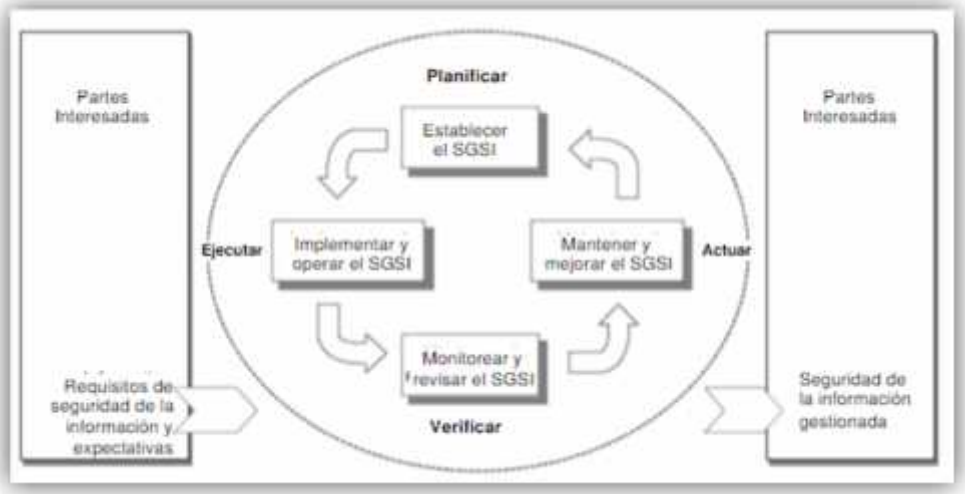




Anexo D. Norma ISO 27001 del Sistema de Gestión de Seguridad de la Información

ISO/IEC 27001 fue elaborada por el Comité Técnico Conjunto ISO/IEC JTC 1, Tecnología de la Información, Subcomité SC 27, Técnicas de Seguridad Informática.

Esta Norma Internacional se ha elaborado con el fin de proporcionar un modelo para establecer, implementar, operar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debería ser una decisión estratégica para una organización. El diseño y la implementación del SGSI de una organización están influenciados por sus necesidades y objetivos, los requisitos de seguridad, los procesos empleados y el tamaño y estructura de la organización. La Norma ISO/IEC 27001 adopta el modelo "Planificar-Ejecutar-Verificar-Actuar" (PDCA), que se aplica a la estructura de todos los procesos del SCSI.



Planificar (Establecer el SGSI)	Establecer la política, objetivos, procesos y procedimientos del SGSI relacionados con la gestión de riesgos y la mejora de la seguridad de la información de una organización.
Ejecutar (Implementar y Operar)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (Monitorear y Revisar)	Evaluar y cuando sea aplicable, medir el desempeño de los procesos en relación con la política, objetivos y experiencia práctica en materia de SGSI.
Actuar (Mantener y Mejorar)	Tomar las acciones correctivas y preventivas, en base a los resultados de la auditoría interna y la revisión del SGSI y otra información pertinente, para lograr la mejora continua del SGSI.

Anexo E. RFC 2196

RFC 2196 (Site Security Handbook) es una guía para el desarrollo de políticas y procedimientos de seguridad informática. La idea detrás de este sitio es proporcionar una versión anotada de la RFC 2196 de libre acceso con la referencia a la norma ISO / IEC 27001 para las organizaciones que deseen implementar las mejores prácticas de seguridad, manteniendo una estrecha relación con el estándar ISO / IEC 27001. El ciclo de una política de redacción está dado por: Redacción, Revisión, Aprobación, Publicación y Actualización.